CONNECTIVITY STANDARDS ALLIANCE (CSA)

Connectivity Standards Alliance

Mission: Ignite creativity and collaboration in the Internet of Things, by developing, evolving, and promoting universal open standards that enable all objects to securely connect and interact. We believe all objects can work together to enhance the way we live, work, and play

Key Offerings:

Develop - Create, evolve and manage IoT technology standards through a well-established, collaborative process. We empower companies with practical, usable assets and tools to ease and accelerate development, freeing them to focus on new areas of IoT innovation

Certify - Our strong certification programs help Members avoid unnecessary development cycles, ensure compliance and validate interoperability. Certification and our stamp of approval tells the world they can buy and use certified products and platforms with confidence

Promote

- We are allies for a connected future. Our membership, spanning the global and the IoT value chain, actively seeks to promote the benefits of global, open standards, the value of the IoT to customers and consumers and to break down the barriers to broad access and adoption of IoT technologies and solutions.

Connectivity Standards Alliance Certifications

Certification at a Glance

Validity: Issued certifications remain valid for the lifetime of the product, which becomes immediately eligible to be listed on the Connectivity Standards Alliance database of Certified Products.

Requirements: Certification is available to Connectivity Standards Alliance members. All new product certifications require product testing at a Connectivity Standards Alliance Authorized Test Provider, by an application with the Connectivity Standards Alliance in our Certification Tool.

Costs: The primary costs associated with product certification are the testing fee and the application fee. Please contact an Authorized Test Provider for testing fee quotes.

Timeline: The total duration of the certification process is dependent on several factors, including the length of time required by the chosen test provider for testing and any specific items identified during the application review

Connectivity Standards Alliance Certification Process

1. Become a member of the CSA - Read Connectivity Standards Alliance Policies and Governing Documents and become a member
2. **Request a Manufacturer ID / Vendor ID -** Contact the Alliance Certification Team to reserve your Manufacturer ID or Vendor ID.
3. **Select a Compliant Platform or Network Transport**
4. **Choose a Testing Provider -** Select from Connectivity Standards Alliance authorized Test Providers at locations all around the world
5. **Send Product to be Tested -**After scheduling testing with an Authorized Test Provider, the facility will make arrangements for testing samples and Protocol Implementation Conformance Statement (PICS) documents to be submitted. Test Provider will issue a final report to the Connectivity Standards Alliance when testing is successfully completed
6. **Submit Certification Application -** Complete and submit an application for certification in the Connectivity Standards Alliance Certification Tool. Instructions for requesting a Certification Tool account and creating/submitting applications can be found in the Connectivity Standards Alliance Members Area

Connectivity Standards Alliance Certification Process

7. **Application Pending -** Connectivity Standards Alliance Certification Team will review your application and, if necessary, request action on specific identified items or information required to make a determination of approval or rejection. At any time during this process, you may reach out to the Connectivity Standards Alliance Certification Team with any questions
8. **Upon Approval -** After your product certification is approved, you will receive a formal certificate from the Alliance and may immediately begin using the Certified Product logo. Certified Product logos have usage guidelines that govern how they are used. Please review the applicable sections before affixing. Logos are provided to the applicant's contact for the certification. For more information about Alliance logos and their usage, please contact us

CSA IoT Device Security Specification Version 1.0

CSA IoT Device Security Specification Version 1.0

Created March 18, 2024

Purpose: Define the requirements that must be met by devices within the initial scope of this Specification to be certified under the Alliance Product Security certification and define the baseline security threshold requirements for an Alliance-based device security certification program defined by the Alliance that can be used to certify the security of IoT Devices

Scope: Certifying the security of consumer IoT Devices, contemplating the use of each such IoT Device in an IoT System for consumer use in the smart home, to meet the level current as of June 2023 required by:

- international standards (specifically European Telecommunications Standards Institute (ETSI) EN 303 645 [3] and National Institute of Standards and Technology (NIST) IR 8425 [4]); and
- regulations (specifically Singapore Cybersecurity Labeling Scheme (CLS) [5]); and
- the markets

Does not cover home healthcare products

CSA IoT Device Security Specification Version 1.0 Key Definitions

- **Best Practice Cryptography -** Cryptographic Algorithms, modes and protocols, key generation and handling, and random number generation required by any government or regulatory body in the applicable market, or markets, in which the IoT Device is intended to be deployed. The choices may be determined by the need for interoperability as required by established specifications as described in section on Best Practices for Cryptography of the PSWG Assessment Guidance
- **Critical Security Parameters -** Security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs), the disclosure or modification of which can compromise the security of an IoT Device.
- **Cryptographic Algorithms -** Cryptographic primitives and higher-level algorithms that perform functions essential to maintaining cryptographic security.

CSA IoT Device Security Specification Version 1.0 Key Definitions

- **IoT Associated Service -** Software that complements an IoT Device, providing an external service that is not executed within the IoT Device.
- **IoT Device -** A tangible product, composed of IoT Sub-Components, that comprises at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world. PSWG 1.0 is limited to devices intended principally for consumer use in the home (excluding home healthcare devices).
- **IoT Device Manufacturer -** An organization that designs, develops, manufactures or markets an IoT Device.
- **IoT Sub-Component -** The underlying hardware/firmware/software from which an IoT System Component is built
- **IoT System -** A collection of related IoT System Components, including IoT Devices and IoT Associated Services. There is no assumption in this Specification that all of the IoT System Components in an IoT System come from the same vendor.
- **IoT System Component -** An IoT Device, an IoT Associated Service, or other equipment used to create an IoT System instance. An example of other equipment would include a router.

CSA IoT Device Security Specification Version 1.0 Key Definitions

- **Security-Related Configuration -** The configuration for security countermeasures for an IoT System or IoT System Component that facilitates the management of risk.
- **Security-Relevant Information -** Information that could identify the combination of the IoT Device and the version of that IoT Device's software and/or hardware.
- **Security Best Practices -** These are the best practices for IoT Device security:
  1. Perform a risk analysis and threat model for the IoT Device in light of the expected usage and target deployment context
  2. Identify and classify data storage points and data flow assets, and safeguard assets classified as Sensitive Data in a manner that satisfies some or all of the following: availability, integrity, and confidentiality, as applicable to each asset
  3. Select appropriate countermeasures to reduce residual risk to acceptable levels
  4. Implement the selected countermeasures.
- **Sensitive Data -**Data that is of particular concern from a security perspective, including, by way of example and without limitation: safety- and/or control-related commands/functions or parameters; data strings; data attributes; personal identifiable information; data in memory being used for calculations; credentials; keys; protocol header fields; and intellectual property

CSA IoT Device Security Specification Version 1.0 Key Technical Requirements

Unique Identity

- The IoT Device SHALL be uniquely identifiable for cybersecurity purposes. This MAY require a set of identities depending upon the specific use.

IoT System Inventory

- If the IoT Device is able to collate or store an inventory of connected IoT System Components, the IoT Device SHALL uniquely identify each such IoT System Component and maintain an up-to-date inventory.

Authentication for Configuration Changes

- If the IoT Device makes or allows Security-Related Configuration changes, including Critical Security Parameters and passwords, via a network or other interface, the related configuration changes SHALL only be accepted after authentication and authorization. Best Practice Cryptography SHALL be used.

Configuring IoT System Components

- If the IoT Device is able to configure other IoT System Components within an IoT System instance, it SHALL be demonstrated that any changes are applied to the other IoT System Component(s). If the IoT Device is able to be configured by other IoT System Components within an IoT System instance, it SHALL be demonstrated that any changes are actually applied in the IoT Device and reflected in the other IoT System Component(s). This requirement only applies to Security-Related Configuration changes.

CSA IoT Device Security Specification Version 1.0 Key Technical Requirements

Uniqueness

- If the IoT Device makes use of Critical Security Parameters, including passwords and identities, they SHALL be unique per IoT Device at the time it is manufactured and SHALL NOT be resettable to any universal factory default. It follows that Critical Security Parameters SHALL NOT be embedded in source code.

  Critical Security Parameters provided by the IoT Device Manufacturer SHALL NOT be easily determined by automated means or obtained from publicly available information or derivatives from fixed parameters associated with the IoT Device.

Security Best Practices

- If the IoT Device makes use of Critical Security Parameters, including passwords, they SHALL conform with Security Best Practices, including, length, complexity, generation of keys from passwords, secure management processes, and secure storage. Best Practice Cryptography SHALL be used.

Preventing Brute Force Attacks

- The IoT Device SHALL implement a mechanism that protects against brute force authentication attacks.

Changing Authentication Values

- If the user can authenticate against the IoT Device, at least the IoT Device or some other IoT System Component SHALL include a mechanism for simply changing user authentication values.

CSA IoT Device Security Specification Version 1.0 Key Technical Requirements

Cryptographic Agility

- The IoT Device SHOULD support updating Cryptographic Algorithms and primitives.

Secure Storage of Persistent Data

- All Sensitive Data stored persistently on the IoT Device SHALL be stored in a secure manner consistent with Security Best Practices.

Erasure from Device

- The IoT Device SHALL support the erasure of local data that is from or about the user which may include personal data about the user, their home or family, user configuration, and cryptographic material.

  Any such erasure, including through a Factory Reset, SHALL be authorized, and SHALL leave the IoT Device in a secure state.

  Note: Requirements related to deleting data outside the IoT Device are not in the scope of this Specification

Restricting Access to Security-Relevant Information

- The IoT Device SHALL require authentication and authorization when exposing Security-Relevant Information via the network interfaces of the device.

Confidentiality Protection

- The IoT Device SHALL, by default, ensure the confidentiality of Security-Relevant Information and Sensitive Data exchanged with IoT Devices and IoT Associated Services. Best Practice Cryptography SHALL be used

CSA IoT Device Security Specification Version 1.0 Key Technical Requirements

Remote Trust Relationships

- For two-way communication, the IoT Device SHALL establish a trust relationship ensuring that both parties at each end of a network connection are authenticated. Best Practice Cryptography SHALL be used.

Disabling Unused Interfaces

- The IoT Device SHALL disable all interfaces not necessary for the intended use of the IoT Device.

Input Data Validation

- Data input into the IoT Device via network and any other interfaces SHALL be validated against malformed input.

Restrict Unused Functionality

- Functionality not needed for the intended use of the IoT Device SHALL NOT be installed, or SHALL be disabled where non-installation is not practical

Least Privilege

- All IoT Device software SHOULD be executed with the lowest possible level of privilege necessary for the intended function.

Secure Boot

- The IoT Device SHOULD perform a secure boot process, using Security Best Practices

CSA IoT Device Security Specification Version 1.0 Key Technical Requirements

Verification of Software Updates

- The IoT Device SHALL support a software update process and SHALL ensure the authenticity and integrity of software updates. Best Practice Cryptography SHALL be used.

Automatic Software Updates

- Automatic software update installation methods SHOULD be employed for updating the IoT Device. The IoT Device SHOULD check for available updates at least once after initialization and then periodically.

Ease of Software Update Installation

- Software updates for the IoT Device SHALL be easy for users to install.

Enablement of Software Updates

- If the IoT Device supports automatic updates and/or update notifications, these SHOULD be enabled by default but an authorized entity SHOULD be able to enable, disable, or postpone installation of security updates and/or update notifications.

Audit Logging

- The IoT Device SHOULD support audit logging of security-relevant events and errors. The log SHOULD include enough details to determine what happened.

CSA IoT Device Security Specification Version 1.0 Key Technical Requirements

Reporting Security State

- The IoT Device SHOULD be able to report the current security-related state

Reporting Unauthorized Software Changes

- If the IoT Device detects an unauthorized change to the software, it SHOULD limit connectivity to the minimum required to report the error to authorized recipients. Detection mechanisms include secure boot, or regular monitoring.

Protected Access to Logs

- If the IoT Device supports an audit log as described in Section 5.5.6.1, Audit Logging and that audit log is stored on the IoT Device, it SHOULD restrict access to the log files to authorized personnel only for defined purposes.

Recovery from Power Failure and Network Outage

- The IoT Device SHOULD be resilient to power and network outages. There SHOULD be no impact on the IoT Device security. The effects of an internet connection outage SHOULD be minimized as much as possible to establish continued local functional operation. After the outage is ended, the IoT Device SHOULD gracefully recover to its normal operational state

Isolation of Processing

- The IoT Device SHOULD make use of isolated processing approaches employing both software-based and hardware-based mechanisms, using best practices and in support of the principle of least privilege.

CSA IoT Device Security Specification Version 1.0 Key Non-Technical Requirements

Design Considerations

- The IoT Device Manufacturer SHALL document the expected usage and target deployment context relating to the IoT Device, including at least:
  - Expected customers and use cases, including known potential misuses
  - Laws and regulations that must be complied with
  - Expected device lifespan
  - Expected cybersecurity costs for the end users
  - Intended security context, including assumed cybersecurity requirements and physical
  - environment
  - Threat model
  - Risk analysis

Development Processes, Platforms, and Tools

- The IoT Device Manufacturer SHALL document the processes, platforms, and tools used to develop the IoT Device, including at least:
  - Platforms and tools
  - Accreditation, certification, and/or evaluation results for these processes, if any
  - Other aspects of development processes related to IoT Device Security, including, by way of example, activities taken under the Development Process Related to IoT Device Security section

CSA IoT Device Security Specification Version 1.0 Key Non-Technical Requirements

Secure development processes are fundamental to IoT Device security. Thus, these requirements for secure development processes are included.

Threat Modeling

- The IoT Device Manufacturer SHALL conduct threat modeling to identify, analyze, and mitigate relevant threats.

Secure Engineering Approach

- The IoT Device Manufacturer SHALL employ a secure engineering approach.

IoT Sub-Components

- The IoT Device Manufacturer SHALL maintain an inventory of IoT Sub-Components used in the IoT Device, including version as well as applied patches and updates.

Hardware/Software Supply Chain

- The IoT Device Manufacturer SHALL implement and maintain the IoT Device using IoT Sub-Components from a secure supply chain, with a risk-appropriate process for addressing vulnerabilities

CSA IoT Device Security Specification Version 1.0 Key Non-Technical Requirements

History has shown that diligent vulnerability management and response is critical for cybersecurity. Thus, these requirements and recommendations are included.

Vulnerability Disclosure

- The IoT Device Manufacturer SHALL establish, publicize, and implement a vulnerability disclosure process for the IoT Device.

  This process SHALL include at least a documented method for reporting issues as well as a timeline for acknowledging receipt of a report and for providing status updates on the resolution of the reported issues.

Vulnerability Response

- The IoT Device Manufacturer SHOULD continually monitor, identify, and respond in a timely manner to security vulnerabilities throughout the defined support period.

Vulnerability Assessment

- The IoT Device Manufacturer SHALL conduct penetration testing or vulnerability testing or both periodically, including at least before every major release.

Security Updates

- Security updates are changes that mitigate or fix security vulnerabilities and follow Security Best Practices

CSA IoT Device Security Specification Version 1.0 Key Non-Technical Requirements

Timely Updates

- The IoT Device Manufacturer SHALL provide timely security updates during the defined support period for the IoT Device.

User Notification of Updates

- The IoT Device Manufacturer SHOULD ensure that the user is notified when a security update is needed, including information about the risks mitigated by the update. If the update will disrupt the IoT Device's functionality, this SHOULD be disclosed.

When Updates Cannot Be Provided

- When updates cannot be provided, the IoT Device Manufacturer SHOULD clearly explain to users why no updates are available, how affected hardware can be isolated and replaced, and the defined support period

Consumer Disclosure

- The IoT Device Manufacturer SHALL provide information to consumers about what personal data (and telemetry data, if any) is being processed, how it is being used, by whom, and for what purposes.

Consent

- When consumer consent is obtained for personal data processing, this consent SHALL be obtained in a valid manner. Consumers SHALL have the power to withdraw this consent at any time.

CSA IoT Device Security Specification Version 1.0 Key Non-Technical Requirements

Minimization

When data is collected from IoT Devices, that data SHALL be kept to the minimum necessary for the intended functionality.

Non-compliance with Requirements or Recommendations

If any provision (requirement or recommendation) in this Specification is not met, the IoT Device Manufacturer SHALL document why this is an appropriate decision based on design assumptions such as the expected use cases, intended security context, and the threat model. Justifications SHALL be based on risk and Security Best Practices not just on cost or previous design decisions.

Compliance with an established specification for the ecosystem in which the IoT Device is intended to be deployed, e.g., for interoperability, may be required. In these circumstances, it is possible that certain requirements cannot be met in order to comply with that specification. In these circumstances, justification for non-compliance SHALL be provided.