App Defense Alliance

Certification Scheme Overview

Contents

Introduction

About the App Defense Alliance Certification Scheme

This document provides an in-depth look at the App Defense Alliance Certification (ADA Certification) Scheme, a comprehensive security certification program designed to elevate industry-wide security standards.

The primary purpose of ADA Certification is to establish a unified security assurance framework that promotes transparency and enhances security functionality within applications. The ultimate goal of this scheme is to drive improvements in security across the entire application ecosystem, ensuring a safer experience for users.

Upon implementation, the ADA Certification Scheme will comprise two primary elements:

1. Security Evaluations: Authorized ADA Security Test Laboratories (ASTL) will conduct thorough security evaluations of applications. These evaluations will be overseen by a designated Certification Body (CB), which is appointed by the ADA to ensure compliance with the scheme's requirements, including quality and impartiality.
2. Evaluation Criteria: Applications will be assessed against the ADA's Application Security Assessment (ASA) requirements. These requirements are developed through an open and collaborative process that draws from reputable industry sources, including:
    a. The Open Worldwide Application Security Project (OWASP)
    b. The Center for Internet Security (CIS)

By leveraging these respected sources and maintaining transparency throughout the development process, the ADA ensures that its ASA requirements reflect the most up-to-date and effective security standards in the industry.

Stakeholder Benefits

The ADA Certification Scheme aims to ensure the safe handling of confidential data by setting a baseline of requirements for organizations that build apps that process such data and with a focus on mobile, web, and cloud applications. The scheme serves to:

1. **Reduce Unauthorized Access to Confidential Data**: By creating a prescriptive set of security best practices, ADA helps organizations that choose to adopt these practices to prevent data breaches and unauthorized access to confidential information.
2. **Increase Trust in Application Platforms**: Sensible and consistent minimum security standards across application platforms builds trust among consumers.
3. **Support Developers With an Ecosystem of Security Assessors**: ADA provides a common framework for mobile,web, and cloud security, allowing Developers around the world to work with qualified security organizations to certify their compliance with the ADA's requirements.

Document Scope

This document has been produced for stakeholders to familiarize themselves with the ADA Certification Scheme. It provides an overview of the scheme, which enables participating Developers to demonstrate that a particular application has achieved an industry-recognized level of security. Applications that satisfy the evaluation criteria will receive a public certificate that is valid for a period of time and describes the security credentials of the application.

This document describes the most important aspects of the scheme, including security assurance levels, the certification process and the validity period.

Document Maintenance

The ADA Certification Scheme documentation was created and developed by the ADA's Steering Committee, composed of representatives from Google, Meta and Microsoft. This group is responsible for ongoing maintenance and development of the ADA Certification Scheme documents and facilitating periodic reviews involving relevant stakeholders.

Abbreviations

App Defense Alliance (ADA)

App Defense Alliance Certification Scheme (ADA Certification)

ADA Security Test Laboratories (ASTL)

Center for Internet Security (CIS)

Certification Body (CB)

Open Worldwide Application Security Project (OWASP)

Security Assurance Level 0, Self Attestation (AL0)

Security Assurance Level 1: Verified Self Assessment (AL1)

Security Assurance Level 2: Lab Assessment (AL2)

Scope of the ADA Certification

ADA Certification is specifically developed s a security assurance scheme in the contex of the environment in which the scheme operates. In particular::

- Mobile and web application frameworks and languages
- Secure configuration of cloud infrastructure
- Visibility of security assurance levels
- Market acceptance and participation

The certification of an application applies either to its default configuration, provided it meets the required security standards, or to a secure configuration process based on the developer's guidelines or instructions.

The certification scheme does not cover user actions that can potentially compromise the security of the application. The following examples illustrate user behaviors that are outside the scope of this certification:

- Compromising security credentials: Sharing passwords or other sensitive information with third parties, whether intentionally or unintentionally.
- Neglecting security updates: Failing to install security-critical updates in a timely manner or blocking their installation, which can leave the application vulnerable to known threats.
- Overriding default security settings: Intentionally or unintentionally granting insecure permissions to applications that were blocked by default in the certified configuration, thereby weakening the application's security posture.
- Using insecure networks: Accessing the application over high-risk networks, such as public Wi-Fi hotspots (e.g., airport Wi-Fi), which may be more susceptible to interception or eavesdropping.
- Disabling security features: Intentionally disabling built-in security functionality, such as password protection, which can significantly increase the risk of unauthorized access to the application.

ADA Certification Scheme Overview

The ADA Certification Scheme provides a valuable opportunity for participating developers to demonstrate their commitment to security by achieving an industry-recognized level of security for their applications. Here's how it works:

- Security Evaluation: Developers can submit their applications for evaluation at one or more security assurance levels.
- Time-Limited Certificate: Applications that pass the evaluation receive a time-limited certificate, which confirms compliance with the specified security standards.
- Security Credentials: The certificate serves as proof of the application's security credentials, providing transparency and assurance to users.

Participation in the ADA Certification Scheme is entirely voluntary, allowing developers to choose which applications they want to undergo security evaluation. This flexibility enables developers to prioritize their applications' security needs and demonstrate their dedication to delivering secure products to their users.

ADA Certification Roles

The ADA Certification Scheme involves several key actors that work together to ensure the scheme's success. These actors and their roles are outlined below:

Scheme Owner	ADA is the Scheme Owner and will own and update the scheme requirements, assurance levels, evaluation methodology, and lab authorization criteria.
Certification Body (CB) / Scheme Operator	ADA will select an ISO 17065 accredited Certification Body (CB), sometimes referred to as the Scheme Operator. The scheme CB will authorize and onboard independent ADA Security Test Laboratories (ASTLs), review evaluations of developer apps submitted by the ASTLs, issue and publish certificates, and operate the related surveillance processes.
ADA Security Test Laboratory (ASTL)	Independent organizations who desire to perform ADA Certification evaluations will engage with the CB to become authorized as an ASTL. ASTLs are required to: (a) have and adhere to the ISO 17025 standard when performing ADA Certification evaluations, and (b) demonstrate technical proficiency in conducting ADA evaluations by successfully passing a proficiency exam administered by the CB. ASTLs submit completed app evaluations to the CB for review. ASTLs that fail to uphold the quality standards of the ADA Certification Scheme will lose their authorization and no longer be allowed to conduct ADA evaluations.
Application Developer	Developers who wish to obtain an ADA Certification will select an authorized ASTL, security assessment level, and set of ADA security profile(s) to be evaluated against. The developer will then provide information, evidence, and access to the ASTL, as necessary, to complete the Lab's evaluation. If the Developer's application, along with supporting information, are sufficient for the Lab to evaluate and establish that each ADA Certification requirement is met, the lab will prepare a passing evaluation report to the CB, which will then issue and publish a time-limited certificate to the developer stating that the app is ADA Certified. During the validity period, if the developer fails to keep the app compliant with the ADA requirements, the CB will revoke the certificate.

The roles and responsibilities of these actors are described in more detail below.

Scheme Owner

As the Scheme Owner, ADA plays a crucial role in managing the ADA Certification Scheme. The following sections outline ADA's responsibilities:

Defining Security Requirements

ADA's Application Security Assessment Working Group (ASA WG) is responsible for defining prescriptive security requirements. These requirements are then reviewed by ADA's Steering Committee, which decides whether to officially release them as alliance standards. Once released, these standards become an integral part of the ADA Certification Scheme.

Maintaining Scheme Documents

ADA is responsible for maintaining the Scheme documents, ensuring they remain up-to-date and relevant.

Key Responsibilities

As the Certification Scheme Owner, ADA's key responsibilities include:

1. Managing Industry Group: Overseeing an industry group that maintains and evolves the Scheme requirements.
2. Maintaining Scheme Documents: Ensuring that ADA Certification Scheme documents are accurate, up-to-date, and readily available.
3. Market Feedback Process: Managing a market feedback process to gather input from stakeholders and maintain the Scheme's relevance and effectiveness.
4. Appointing a Competent CB: Selecting a competent Certification Body (CB) and ensuring their adherence to the ADA Certification Scheme requirements.

By fulfilling these responsibilities, ADA ensures the overall direction and operations of the Scheme align with its goals and objectives.

Certification Body (CB) / Scheme Operator

The ADA Certification Scheme is designed to operate in accordance with the provisions and expectations of ISO 17065. Certification Body (CB) is responsible for:

- Gaining and maintaining ISO 17065 accreditation to participate and provide certification services for the scheme
- Identifying necessary updates to ensure ongoing alignment between ADA Certification and ISO 17065 expectations
- Agreeing to terms and conditions for participation in the scheme

The CB shall specifically include the ADA Certification scheme within the scope of their ISO 17065 accreditation/certification process.

The CB is responsible for, among other things:

- Authorizing, supporting and monitoring the performance of ADA Security Test Labs (ASTLs)
- Ensuring ASTLs' competence in conducting ADA evaluations and their adherence to the ADA Certification Scheme requirements
- Managing the ADA Certification Scheme dispute resolution process
- Certification activities, including
    - Publishing certificates
    - Maintaining an archive of historical certification data
    - Certificate lifecycle tracking (e.g., Valid, Expired, and Revoked)

The Scheme Owner's website shall publish the primary point of contact's information for the ADA Certification scheme at the CB, along with details about authorized ASTLs and ADA Certification Scheme

policies and procedures documents. The Scheme Owner is responsible for oversight of the CB to ensure consistency across evaluations performed by the ASTLs.

ADA Security Test Laboratory (ASTL)

ASTLs are authorized to perform application evaluations by the CB. For laboratories to become, and stay, authorized under the scheme, they need to:

1. Petition to become an ASTL
2. Begin the ISO/IEC 17025 Certification Process and successfully complete the process within a year of applying
3. Demonstrate technical proficiency in conducting ADA evaluations by successfully passing a proficiency exam administered by the CB.
4. Completion of the ISO/IEC 17025 Audit

Reference the ADA Lab Authorization document for details.

Candidate ASTLs wishing to be authorized should contact the CB and be prepared to provide evidence of how the above requirements are met. Organizations that successfully petition to become ASTLs will be listed by the Scheme Owner as such under the ADA Certification Scheme.

Application Developer

To obtain an ADA Certification for one or more applications, developers must follow these steps and fulfill the associated responsibilities:

Step 1: Select an Authorized Lab and Agreeing to Terms

- Choose an authorized ADA Security Test Laboratory (ASTL) to conduct the evaluation.
- Agree to the terms and conditions of the relevant actors, including non-disclosure agreements (NDAs), to participate in the Scheme.

Step 2: Select Applications and Evaluation Scope

- Identify one or more applications to be evaluated by the ASTL.
- For each application, specify:
    - The desired security assurance level (e.g., AL0, AL1, or AL2).
    - The relevant ADA requirements profile(s) (e.g., mobile, web, cloud, or a combination).

Step 3: Provide Required Information and Assistance

- Supply the ASTL with all necessary information, evidence, and access required for the chosen security assurance level and profile(s).
- Assist the ASTL and Certification Body in evaluating and certifying the application.
- Provide transparent, comprehensive, and accurate information to the ASTL, including:
    - Descriptions of data flows.
    - Use of external components.
    - Code samples.
    - Other relevant details.

Ongoing Obligations for Certified Products

- If a certificate is granted, the developer must fulfill ongoing obligations to maintain the certification.
- Failure to meet these obligations may result in the revocation of the certificate.

By following these steps and fulfilling their responsibilities, application developers can ensure a smooth and successful ADA Certification process.

ADA Certification Security Requirements

Reference ADA's security requirements on Github at https://github.com/appdefensealliance/ASA-WG

Security Assurance Levels

ADA will have 3 assurance levels that provide increasing levels of rigor in the evaluation and therefore increasing levels of assurance that the product does meet the ADA's requirements.

Description	Level of Assurance	Level of Effort to Obtain Certification	Expected Applicability (Long Term)
AL0 - Self Attestation	Limited	Minimal (hours)	90% of products
AL1 - Verified Self Assessment	Reasonable	Moderate (days)	10% of products
AL2 - Lab Assessment	Advanced	Substantial (weeks)	

AL0 - Self Attestation

A Developer reviews each of the applicable ADA requirements in comparison to their product(s) and, if the developer concludes that their product meets every requirement, makes a fair presentation declaration via a questionnaire (i.e., a self attestation) that their application is compliant with the ADA requirements.

ASTLs express no opinion on whether or not the Developer does comply with any of the ADA security standards.

AL1 - Verified Self Assessment

A Developer performs lightweight testing, typically using publicly available tooling, and provides evidence to an ASTL via a questionnaire. Some developers may enlist an ASTL to conduct the lightweight testing instead of doing it themselves. In either case, the ASTL must review the test results.

Under AL1, the ASTL ensures that:

- The developer has provided enough contextual information about how their product processes confidential data to set the scope of applicable requirements

- The Developer has submitted sufficient evidence to evaluate whether or not the Developer has met each of the applicable requirements for the selected ADA requirements profiles
- The evidence substantiates that the developer has in fact met each of the applicable requirements

This level provides reasonable assurance.

AL2 - Lab Assessment

An ASTL will verify that every security functional requirement is met. The Developer will supply the ASTL with required information, evidence, and access (as required) relevant to the chosen security assurance level and profile(s). The ASTL must ensure that:

- **For requirements that can be tested**:
  - The developer's product is conformant with the ADA requirements
- **For requirements that cannot be tested:**
  - That the developer has submitted evidence necessary to evaluate whether or not the Developer has met the requirement, and
  - That the evidence substantiates that the developer has met the requirement

This level provides the highest level of assurance.

ADA Certification Scheme Process

The ADA Certification Scheme consists of the following phases:

1. Preparation
2. Submission
3. Evaluation
4. Certification

As there are differences between the Security Assurance Levels, differences between the levels at the phases will be noted with ().

Preparation Phase

During the preparation phase, the Developer:

(ALL) Selects the application(s) for evaluation and certification
(ALL) Selects the ADA requirements profile(s) desired for each application
(ALL) Chooses one or more Security Assurance Levels
(ALL) Performs the due diligence to understand their application architecture and flows of confidential data that are relevant for defining the scope of the evaluation
(ALL) Identifies personnel necessary to support the evaluation such that transparent, comprehensive, and accurate information can be provided to the ASTL
(ALL) Agrees to the terms and conditions of participation in the scheme with the Scheme Owner, ASTL and CB, as required
(ALL) Submits the completed intake form
(AL1/AL2) Agrees an expected evaluation duration with the ASTL

(AL2) Prepares credentials (if required) for the ASTL to complete their evaluation (e.g read-only access to cloud accounts)

Submission Phase

During the submission phase, the Developer organizes and submits to the ASTL the following artifacts, as required by the Profile(s) and Security Assurance Level being targeted:

(ALL) the questionnaire (if applicable)
(ALL) any additional evidence documentation and artifacts
(ALL) any recognized security certificates relating to components
(ALL) any recognized security certificates relating to the application
(ALL) justifications of similarity
(ALL) recognized historical certification evidence for re-use
(AL2) Access credentials (if required) for the ASTL to complete their evaluation

Evaluation Phase

The evaluation phase is defined in the ADA Certification Scheme security evaluation methodology and will be applied for Application Evaluations under the Scheme according to the Security Assurance Level applied for by the Developer.

During the evaluation phase, the following actions occur:

(ALL) The questionnaire is reviewed by an authorized ASTL for completeness and accuracy
(AL1) At developer's discretion, either the developer or ASTL conducts lightweight testing of the applications and the ASTL reviews the testing outcomes and completed Developer questionnaire
(AL2) ASTL runs all security tests on the application to validate Developer assertions from the test questionnaire.
(AL1/AL2) ASTL reviews all Developer submitted documentation for completeness and to verify all of the non-technically testable requirements
(AL1/AL2) The ASTL sends requests for more information to the developer if required information (e.g. evidence, samples, etc.) is missing or insufficient for the evaluation to be completed

(AL1/AL2) During the course of the Evaluation, limited remediation work (i.e. documentation updates, applications updates, etc.) may be carried out by the Developer upon a requirement failure.

(ALL) Reporting of results and conclusions from Application Evaluations shall follow the requirements defined in the scheme.

Certification Phase

This phase includes certification Review, Decision and Attestation processes.

If an evaluation is successful, the ASTL sends a completed Evaluation Report to the CB. Incomplete or failed evaluations do not result in an Evaluation Report being to the CB. Instead, the ASTL will send a notice of the termination.

The CB conducts a review of the Evaluation Report's results and the evaluation procedures / testing methods.

During the CB report review, the CB works with the ASTL to resolve any questions or comments. The ASTL can work with the CB (and if necessary the Developer) on addressing any questions or comments (including, as needed, additional testing). At the end of this phase, the CB will prepare a Certification Report – which contains the result of pass, fail, or inconclusive – and deliver it to the Developer, ASTL, and the Scheme Owner.

Passing Certifications will be published by the Scheme Owner with a "valid" designation.

ADA Certification Scheme Certification Decision & Attestation

Certification Decision

-

After the ASTL completes the evaluation, it submits a technical report to the Certification Body (CB) for review. The CB then prepares a Certification Report, which includes a recommendation for certification.

CB's Responsibility

The CB is solely responsible for making the certification decision, which is documented in the Certification Report.

Certification Decision Options

When determining whether an Application complies with the ADA Certification Scheme security requirements, the CB's certification decision will be one of the following:

1. Certified: The Application meets the scheme's rules and policies, fulfills the security requirements, and is certified compliant.
2. Not Certified: The Application is not compliant and is not certified.

Notification of Non-Certification

If the CB decides not to certify the Application, they will identify the reason(s) in the Certification Report and communicate it to both the ASTL and the Developer.

Applicability of Certification Decision

The certification decision applies to various certification processes, including:

1. Initial Certification: Granting certification for the first time.
2. Scope Extension or Reduction: Extending or reducing the scope of an existing certification.
3. Revocation: Revoking an existing certification.
4. Maintenance: Maintaining an existing certification through ongoing evaluation and assessment.

By following this process, the CB ensures that certification decisions are thorough, transparent, and consistent with the ADA Certification Scheme's requirements.

Attestation

If the CB decision is Certified, the CB shall issue an ADA Certification Scheme certificate describing the scope of the Certification, security assurance level, profile(s) and the validity period. This step is dependent upon formal approval of certification by the CB, which includes:

- The Certificate
- The Certification Report

ADA Certification Scheme Certificate Validity Period

The maximum validity of the certification is 365 days from the date of issue, unless there are significant changes to the application that require an updated assessment by the Developer or otherwise invalidate the certification. The renewal criteria for the certification will be determined by the individual platforms that choose to rely on ADA certificates.

Product Changes and Evaluations

ADA specifies the following evaluations based on the level of changes made to the app:

a. Full: This is a complete evaluation. Completion and fulfilling a full evaluation will set a new expiration date of the certification (i.e, 365 days after the date of issuance of a certificate resulting from the full evaluation).
b. Targeted: This is specifically for a patch to fix a critical vulnerability. This evaluation would not extend the expiration date of the previously-issued certification.

It's important to note that these evaluations are based on general guidance and discretion. The Platform may require re-evaluation of the app at any time if it determines that the app is not in compliance with its policies or guidelines.

Change Type	Full	Targeted	No action
New, major version of the app or change of web/cloud architecture / hosting provider	X		
Patching a specific vulnerability reported as part of the market feedback	X	X	
Minor changes such as bug fixes or minor enhancements that do not impact the app's core functionality or user experience			X

Renewing a Product Security Certification

When a Certificate is nearing expiration, the developer must undergo a full re-evaluation of the application to extend its validity period. This process is similar to the evaluation required for a major update to the application.

Streamlined Re-Evaluation Process

While a full re-evaluation is necessary, it's possible to reuse relevant evidence materials from the previous evaluation. This can expedite the re-evaluation process, making it potentially quicker than the initial evaluation. By leveraging existing documentation and evidence, developers can reduce the time and effort required to renew their certification, while still ensuring that their application meets the current security standards.

ADA Certification Scheme Certificate Revocation

The Certification Body (CB) is responsible for managing the issuance and revocation of certificates under the ADA Certification Scheme.

Grounds for Revocation

The CB may revoke a certificate in the following situations:

1. Non-Compliance with Vulnerability and Patch Management Policies: If a Developer fails to follow the vulnerability and patch management policies declared at the time of Certification for a certified Application.
2. Failure to Address Exploitable Vulnerabilities: If a Developer is informed of exploitable vulnerabilities and fails to fix them within a reasonable timeframe (typically 90 days, but no more than 180 days).
3. Failure to Disclose Newly Discovered Vulnerabilities: If a Developer fails to inform the CB of newly discovered exploitable vulnerabilities that impact a certified Application.
4. Deliberate Failure or Violation of Certificate Terms: If the CB considers the Developer's responses to be a deliberate failure or violation of the terms under which the Certificate was awarded.
5. Extraordinary Situations: In severe cases, the CB and Scheme Operator reserve the right to revoke the certification immediately.

Revoked Certificate Status

Once a certificate is revoked, it will be moved to the archive list by the Scheme Owner and designated as "revoked". This ensures transparency and accountability in the certification process.

ADA Certification Mutual Recognition

ADA may decide to recognize certifications from other schemes as equivalent to product certifications performed under the ADA Certification program. Recognition may be done by the ADA at the program level such that all certifications from the external certification program are automatically recognized or on a per-application basis at the request of the developer. In the future, the ADA may elect to recognize other certificate schemes as equivalent to the ADA's. If so, the ADA will update these scheme documents accordingly.

The CB will manage any mutual recognition arrangement with another program, including how to map the certificates into the ADA Certification levels. For individual applications, the CB would ascertain the equivalency of the program and provide a mapping for the certificate.

Evolution of ADA Certification Security Requirements

The ADA Certification security requirements will evolve over time to address changing application capabilities and emerging attack vectors. To ensure clarity and transparency, the requirements will be versioned, and the version used in an evaluation will be clearly denoted on the certificate.

Transitioning to New Requirements

When new requirements are approved, they will supersede the current requirements. To facilitate a smooth transition for Developers, ASTLs, and consumers of certifications, a transition period will be implemented between the old and new sets of requirements.

Transition Period Guidelines

1. Single Set of Requirements: Under normal circumstances, only one set of major release requirements is applicable for an evaluation.
2. Dual Requirements During Transition: When a new set of requirements is published, a six-month transition period begins. During this time, evaluations can start using either the newly released or the next-most-recent major version of the requirements.
3. Retirement of Old Requirements: After the transition period ends, the old set of requirements is retired and can no longer be used for new evaluations.

Certificate Validity

The retirement of old requirements does not affect the validity period of certificates issued using those requirements. Certificates remain valid for their entire defined period unless revoked due to unrelated reasons. This ensures that certified products continue to be recognized as secure, even if the underlying requirements have changed.

ADA Certification Scheme Post Certification Market Feedback Process

a.

Challenging the Validity of an ADA Certification

ADA provides a mechanism for external entities to challenge the validity of an ADA Certification. This process allows for the review of claims or other information relevant to the certification.

Handling Market Feedback and Challenges

The Certification Body (CB) is responsible for documenting and handling market feedback, including challenges to ADA Certifications. The following steps outline the process:

Step 1: Submitting a Challenge

- A challenge is submitted to the CB with sufficient information to identify the ADA Certification being challenged and evidence of non-compliance with security claims.
- Challenges without sufficient evidence will not be reviewed, but additional information may be requested.

Step 2: Initial Review

- The CB conducts an initial review to determine whether the challenge is valid.
- If the challenge is deemed invalid, a response is sent to the submitting party with a reason for rejecting the challenge.

Step 3: Notifying the Developer and Lab

- For valid challenges, the CB contacts the Developer and the lab that performed the evaluation, providing the reasoning for the determination.

Step 4: Developer Response

- The Developer has the opportunity to respond to the valid challenge.

Step 5: Final Determination

- Based on the Developer's response, the CB issues a final determination, which can include:
    - Rejecting the claim
    - Considering the challenge valid but already resolved
    - Considering the challenge valid but unresolved
    - Other possible outcomes as determined by the CB

This process ensures that challenges to ADA Certifications are thoroughly reviewed and addressed, maintaining the integrity and trustworthiness of the certification scheme.

Developer Responses to a Challenge

A Developer may respond to the challenge as they see fit, but some example responses to a VALID challenge are likely to include:

- A counter against the validity of the challenge.

- A patch along with an expected release date for the patch.
- A plan for resolving the challenge (if it is not specifically a product issue).

CB Analysis of Developer Responses

The CB will respond to the Developer's response. Some example responses are:

- Investigate the claim brought forth by the Developer.
- Change the initial review determination (reject the challenge).
- Determine the response resolves the reported challenge and maintains a valid ADA Certification during the remediation process (if remediation is not completed, the certification would be revoked).
- Request further changes to the product based on a review of the response.

CB Revocation of a Certificate

A certification may be revoked when:

- The Developer is unable to provide an adequate resolution of the challenge.
- The Developer does not respond to the challenge inquiry. The CB is responsible for evaluating whether the Developer's response time is appropriate according to industry best practices.

Challenge Constraints

Due to the nature of the Market Feedback Process, the challenge process shall include certain safeguards to prevent abuse. Challenges that are intentionally invalid can tie up resources across the ecosystem, from the scheme to the labs and the Developers. While the initial review process should filter most of these challenges, the following guidelines will assist in limiting abuse:

- A challenge can only be submitted by an organization on an issue one time. Additional challenges on the same issue from that organization will be rejected.
- A Developer cannot challenge another Developer’s product unless said challenge is reported through a group within the challenging organization that specifically publishes security/vulnerability issues.

ADA Certification Scheme Dispute and Interpretation Resolution Process

ADA shall implement a process to resolve disputes (or questions for interpretation) that may arise with regard to the implementation or interpretation of the scheme documentation. It is expected that over time, Developers, labs or other interested parties may have questions regarding the documentation and how it applies in specific situations. In all these cases, a dispute resolution process will be followed.

ADA expects that disputing parties will use good faith and all reasonably available resources to come to a resolution before involving ADA. It is understood that requests for interpretation will generally need to go directly to the ADA, in which case the parties involved shall provide proposed resolutions along with the request for interpretation (though ADA is not obligated to follow any proposed resolution). While the general flow for each process is the same, there are some differences (mainly in terms of who provides the judgment).

Dispute Resolution Process Steps

When a request for dispute resolution is to be made, subject to the conditions laid out, the process is as follows:

1. The requesting party/parties send a written (email or other means specified by the ADA) request for resolution to the ADA.
    a. The request shall include information about the issue being disputed, the reason for the dispute/request, supporting arguments and proposed resolution(s).
2. Upon receipt of the request, the ADA will determine if a similar dispute has been raised and resolved previously.
    a. If a similar dispute has previously been resolved, that outcome would be referenced here and used as the resolution.
    b. If the dispute is new, ADA will inform all relevant parties and allow for comments to be made and discussed. If an agreement is reached here, the process ends.
3. If the parties are still in dispute, ADA will establish a committee of individuals (at least 3) not directly involved with the dispute to judge the dispute.
    a. Each party of the dispute shall appoint one impartial arbitrator, who will then appoint the third impartial arbitrator by agreement.
4. The committee will use reasonable commercial efforts to seek a resolution as soon as practical and without undue delay. A majority decision will determine the resolution of the dispute.
5. ADA will distribute the resolution to the parties involved as well as to the wider ecosystem. This resolution will be binding to all parties.

As resolutions are binding decisions that may lead to results including sanctions such as the revocation of a certificate or loss of authorization of an ASTL. Any sanctions to be imposed are determined as part of the committee decision.

Liability of Resolution Committee Members

Rulings from a resolution committee are undertaken “as is” with no liability to the ADA, committee members, scheme staff or any related members. As a condition to invoking the dispute resolution process, the appellant agrees to hold the ADA, including the resolution committee involved in rendering the decision, harmless from any and all liabilities or damages related to the outcome of the dispute.

Interpretation Resolution Process steps

An interpretation request is generally one where a Developer and lab seek clarification about the requirements provided by the scheme documentation. This type of request usually results in changes to the documentation around the requirements. As the requirements documents may not be changed continually, these interpretations will be published publicly and applied manually until the requirements documentation is updated.

1. The requesting party/parties sends a written (email or other means specified by the ADA) request for resolution to the ADA. The request shall include information about the interpretation being requested, the reason for the request, supporting arguments and proposed resolution(s).
2. Upon receipt of the request, the ADA will determine if a similar resolution has been raised and resolved previously.

    a. If a similar request has previously been resolved, that outcome would be referenced here and used as the resolution.
    b. If the request is new, ADA will review the request and determine the proper interpretation of the requirements.
3. ADA will distribute the resolution to the parties involved as well as to the wider ecosystem.

Matters outside the Scope of ADA Certification Dispute Resolution Process

The processes described here only related to the interpretation and implementation of the requirements laid out in the scheme documentation. Any dispute regarding facts, findings or recommendations of an evaluation report itself shall be resolved between the CB, ASTL and Developer.

ADA Certification Certificate Description

An ADA Certificate shall contain the following minimum information:

- Product name for the application
- Unique identifier established by the certification body issuing the certificate
- Unique identifiers for the evaluated application(s) (e.g.for mobile - application name, namespace, and version)
- Supported/Tested OSes
- Name, address and contact information of the Developer
- Name, address and contact information of the ASTL that performed the evaluation
- Name, address and contact information of the Certification Body that issued the certificate
- Date the evaluation was completed
- Period of validity of the certificate
- Version of the Scheme security requirements
- Assessment Scope (the selected ADA Profiles used in the evaluation)
- Security Level of the evaluation

The Scheme Owner may require additional information.

Annex

Document History

October 1, 2024	v1	First Version
Mar 25, 2025	v1.1	Readability clean up