App Defense Alliance

Evaluation Methodology

Contents

Introduction

This document forms part of the documentation for the App Defense Alliance Certification (ADA Certification) Scheme Methodology.

Document Scope

The evaluation methodology establishes how the product and evidence evaluation is done at the procedural and operational level.

Document Maintenance

The ADA Certification Scheme documentation was created and developed by the App Defense Alliance (ADA), composed of members of Google, Meta and Microsoft. This group will maintain responsibility for ongoing maintenance and development of the ADA Certification Scheme documents and facilitate periodic reviews involving relevant stakeholders.

Abbreviations

App Defense Alliance Certification (ADA Certification)

App Defense Alliance (ADA)

ADA Security Test Laboratories (ASTL)

Certification Body (CB)

Security Assurance Level 0, Self Attestation 0 (AL0)

Security Assurance Level, 1: Verified Self Assessment 1 (AL1)

Security Assurance Level 2: Lab Assessment 2 (AL2)

Developer Evaluation Artifacts

As part of the Application Security Assessment, developers must provide the following information to the ADA Security Test Lab (ASTL):

- All Assurance Levels: A completed questionnaire, which may include both public and confidential information. Note that the public questionnaire will be published as part of the certification.
- Verified Self-Assessment (AL1) and Lab Assessment (AL2): The application(s) to be evaluated.
- Lab Assessment (AL2) only: Access credentials required for testing, such as read-only access to cloud accounts under evaluation.

Confidential Information Handling

If the questionnaire includes confidential information, it can be provided in a separate document. However, the public questionnaire must contain high-level answers to every question. The Certification Body (CB) reserves the right to determine if the information provided in the public questionnaire is sufficient.

Multiple Application Evaluations

When multiple applications are evaluated together, the developer must provide justification for their similarities (e.g., common software components) in the questionnaire. This allows the ASTL to assess the applications and their similarities using these components.

Documentary Evidence Requirements

All documentary evidence must be provided in English. Failure to provide complete information will result in an unsuccessful evaluation and certification outcome.

Developer Responsibilities

Developers are responsible for providing transparent, comprehensive, and accurate information to the ASTL throughout the evaluation process.

Evaluation Questionnaire

Questionnaire Requirements

The questionnaire must align with the current set of applicable requirements from the ADA Certification Scheme at the time of application for evaluation. To ensure this, ASTLs must:

- Use the latest major release version of the questionnaire (i.e., not use an obsolete version that has been superseded by a new major release more than six months ago)
- Incorporate changes from minor releases of the ADA requirements within 30 days of the minor release

Certification and Public Disclosure

Upon successful completion of the certification process, the certificate will be made publicly available by the Scheme Owner, along with the completed questionnaire. Developers must provide necessary confidential or proprietary information as supplemental evidence, with high-level summaries included in the questionnaire.

Security Assurance Levels

The following Security Assurance Levels require different levels of evaluation:

- Security Assurance Level 0 (AL0): Self Attestation
  - Developers review applicable ADA requirements and confirm their product meets every requirement
  - Developers complete a questionnaire to represent their application's compliance with ADA requirements
  - Developers guarantee the completeness and accuracy of the questionnaire
- Security Assurance Level 1 (AL1): Verified Self Assessment
  - Developers perform lightweight testing using publicly available tooling and collect evidence in a questionnaire
  - Developers can choose to engage an ASTL to assist with testing
- Security Assurance Level 2 (AL2): Lab Assessment

  - The ASTL tests technically testable security requirements and reviews Developer-provided documentation
  - Developers complete a questionnaire for items that the ASTL cannot evaluate on their own

Testing and Verification

When performing testing, Developers must provide sufficient detail for the ASTL to verify that the tests accurately demonstrate the implementation and compliance with ADA Certification security requirements. If external testing is used, the results must be publicly available and verifiable by the ASTL. The Developer must explain how the external testing demonstrates compliance with ADA Certification security requirements. The ASTL reserves the right to reject test evidence if it cannot confirm compliance with a specific ADA Certification security requirement.

Providing Application-Related Documentation Evidence

The questionnaire shall contain sufficient public information to demonstrate compliance with ADA Certification security requirements. When information that shall remain confidential is necessary to provide additional details, that information may be submitted in a separate form or questionnaire and should be clearly associated with the relevant ADA requirements.

To support a developer's claims and enhance the understanding of the applications under evaluation, developers can provide various types of documentary evidence. The format and documents are flexible, but the following examples illustrate the types of information that can be useful:

- Attachments: Include files such as:
  - Android Manifest or Info.plist
  - Screenshots of app settings, configurations, or features
  - Design documents explaining data encryption, key management, authentication protocols, source code quality, and compiler security features
  - Reports generated by tools like mobsf, objection, and semgrep
- Screenshots: Provide images showing specific aspects of the app, such as:
  - Input typing and UI elements
  - Permission requests and authorization flows
- Design documents: Write explanations of how certain features or mechanisms work within the app, including:
  - Data encryption and key management
  - Authentication protocols and session management
  - Source code quality and compiler security features
- Code snippets: Share portions of code that demonstrate the implementation of security controls, such as:
  - Password storage and verification
  - Session management and authentication
- Log samples: Provide examples of log files that demonstrate the application's logging practices, such as:

    - Not writing sensitive information into logs
- Tool output: Include results from running specific tools, such as:
    - Mobile tools (e.g., semgrep, objection, mobsf) that provide information about the app's security posture
    - Dependency scans that identify vulnerabilities in third-party libraries used by the application
    - Cloud CLI output relevant to the secure configuration of cloud assets
- Justifications: Offer explanations for design choices or configurations that may not align with security best practices

Applications for Evaluation

The expectation is that the Developer provides a production version of their application and the application relies upon a trustworthy computing platform that runs a recent version of an operating system (i.e. N-3). When access to the production version of the app is not feasible, an alternative version may be tested (i.e. testing a web application in a non-production environment, testing a non-production mobile application with certain security mechanisms disabled, etc.)

The ASTL is responsible for ensuring that the tested version or environment is identical to the one used in production.

Platforms for Evaluation

It is the responsibility of the ASTL to have the necessary tools available to perform evaluations. The ADA will not be involved in the distribution of devices/hardware.

Evaluation Methodology

The three security assurance levels of the ADA Certification Scheme generate different levels of output corresponding to the activities mandated at each level. The table below describes the evaluation report contents associated with each assurance level:.

Security Assurance Level	**Evaluation Report Content**
AL0 - Self Attestation	Questionnaire Evaluation report
AL1 - Verified Self Assessment	Questionnaire Evaluation report Evaluation Reports Vulnerability Analysis Report*
AL2 - Lab Assessment	Questionnaire Evaluation report

	Evaluation Reports Security Testing report Vulnerability Analysis Report*

*The input for this analysis can come from OWASP dependency check or other ADA approved scanning tool

The evaluation process and reports are described in more detail in the following sections.

Evaluation Process

After receiving the required evidence artifacts from the Developer, the ASTL follows these steps to evaluate the application:

1. Initial Review: The ASTL conducts an initial review of the submitted material to ensure it meets the requirements.
2. Request for Additional Information: If necessary, the ASTL requests missing or additional information from the Developer within an agreed-upon time limit.
3. ASTL Determines Evaluation Outcome: If the ASTL finds that the evaluation outcome is “Pass” then the ASTL proceeds to the next step. If the evaluation outcome is "Fail", the ASTL informs the Developer, who then has two options:
    - Withdraw from the evaluation process
    - Provide mitigation(s) or resolution(s) to address the identified issues
4. Compilation and Submission of Reports: The ASTL compiles the Questionnaire Evaluation and Security Testing Reports and submits them to the Certification Body (CB).
5. CB Determines the Certification Outcome: If the CB decides that the outcome is “Pass” then the CB proceeds to the next step. If the outcome is "Certification Fail", the CB informs the ASTL and the Developer, who again has two options:
    - Withdraw from the evaluation process
    - Provide mitigation(s) or resolution(s) to address the identified issues
6. Certification Awarded: If the CB assessment results in certification, the results are shared with the Developer for their records and with the Scheme Owner for publishing.

Evaluation Activities

The duration of the various ADA Certification evaluation activities are:

- Defined in the ADA Certification Scheme Terms and Conditions by the ASTL, CB and Scheme Owner, and

- Agreed to by the participating Developer

These terms may include service level agreement targets and rules for extensions or remediation work.

If, during the evaluation process, the Developer needs to request additional time to successfully complete the evaluation, a pause in the evaluation may be requested, subject to agreement by the ASTL and ASCB. This can provide the Developer with the time necessary to complete remediation for failures that may be reported during the evaluation process (instead of withdrawing from the evaluation).

Evaluation Reports

There are four separate reports that may be generated in an evaluation. The specific reports depend upon the security assurance level of the evaluation. Each report contains a number of predefined sections which shall be completed by the Evaluator.

Questionnaire Evaluation Report

The Questionnaire Evaluation Report shall contain the following sections:

1. Introduction
    a. Identify the Applications under evaluation
2. Questionnaire review results
    a. PASS/FAIL/INCONCLUSIVE results for all ADA Certification requirements
3. Conclusion
    a. Final recommendation based on the information provided in the questionnaire
4. Bibliography
    a. Reference list to all information used in the evaluation process

Security Testing Report

The Security Testing Report shall contain the following sections. It is noted these are just the sections but there could be additional information included in the reports.

1. Introduction
    a. Test objectives and summary
2. Test platforms and environments
    a. Application version information (detailed)
    b. Test environment
    c. Testing tools
3. Test case description
    a. Description of each individual test and outcome of the test
4. Conclusion
    a. Final recommendation based on the results of the security testing

Vulnerability Analysis Report

The Vulnerability Analysis Report shall contain the following sections:

1. Introduction
    a. Test objectives and summary
2. Vulnerability analysis

3. Public vulnerability search
    a. Keywords, search terms, findings in NVD
    b. Descriptions of excluded vulnerabilities
    c. Table with findings
4. Conclusion
    a. Final recommendation based on the results of the vulnerability search analysis
5. Bibliography
    a. Reference list to all information used in the analysis

Evaluation Report

The Evaluation Report shall contain the following sections:

1. Introduction
2. Developer information and Application reference
    a. TOE version information (detailed)
3. Evaluation Result
    a. Summary of questionnaire review result
    b. Summary of security testing result
    c. Summary of vulnerability search analysis result
4. Overall verdict
5. Lab recommendations
6. Bibliography

Assessment Verdicts in the Technical Reports

All Technical Reports contain the verdicts for the ADA Certification security requirements (as appropriate to the Technical Report). While the final versions of the Technical Reports may only include PASS/FAIL verdicts, interim reports may also include INCONCLUSIVE verdicts.

For the Developer to successfully complete the ADA Certification evaluation, the Technical Reports can only include PASS verdicts for the individual requirements. Generally, the Developer is expected to correct any issues that result in a FAIL or INCONCLUSIVE verdict such that the Application will receive a PASS verdict for the completion of the evaluation.

During the evaluation process, the ASTL shall provide the Developer with updates about interim verdicts so they can be remediated as necessary. The ASTL shall determine whether a remediation is sufficient to change the verdict to a PASS.

When a remediation is provided to resolve a non-PASS verdict, the Developer shall provide an explanation of the scope of the remediation so the ASTL can determine whether additional re-testing is required (e.g., if the change impacts other aspects of the security claims under review). Insufficient information from the Developer may lead to longer test times or a continued FAIL verdict.

Evidence Assessment

Questionnaire Assessment

The assessment of the questionnaire is completed by the Developer. It is submitted to the Lab where it is reviewed and then submitted to the CB who determines if it is complete, consistent, and accurate:

- Completeness:
  - The Evaluator shall check that the information uniquely identifying the applications for certification has been included.
  - The Evaluator shall check that all ADA Certification security requirements have been addressed by specific security functions and that the necessary supporting evidence has been submitted.
  - In the event that the Developer considers that a security requirement is not applicable to an application, given its purpose or available interfaces, the Developer shall provide a justification. The CB shall make a determination whether each such claim (and omission of evidence) is compatible with the scheme and enables the application to be certified subject to successful outcomes of the other activity evaluations.
- Accuracy:
  - The Evaluator shall check that the information provided by the Developer is accurate compared with the results of security testing performed during the evaluation.
  - The Evaluator shall check that the descriptions faithfully describe what is implemented.
- Consistency:
  - The Evaluator shall check that the information does not provide divergent or conflicting answers to separate security requirements.

Assessment Verdicts

The verdicts of the testing include: PASS/FAIL/INCONCLUSIVE

Security Testing

Security testing is a process that verifies the features and functions of a product are working as intended and protecting against potential vulnerabilities or attacks. ASTLs must follow the ADA's test guides and acceptance criteria to ensure the product meets the ADA's security standards.

In some cases, developers may use alternative approaches to meet individual requirements, and it is the responsibility of the ASTL to:

1. Determine if the developer's approach provide equivalent or stronger protection than the default approach described in the ADA test guide, and
2. List and justify each use of an alternative implementation in the resulting evaluation report

Annex

Document History

October 1, 2024	v1.0	First Version
March 25, 2025	v1.1	Revisions per feedback