App Defense Alliance

Security Test Lab Authorization

Contents

Introduction

This document forms part of the documentation for the App Defense Alliance Certification (ADA Certification) Scheme. An overview of this Scheme is available within the ADA Scheme Overview.docx. This Lab Authorization document defines the requirements for ADA Security Test Laboratories and sets the standard against which authorization is to be assessed and awarded and the processes for that authorization.

Document Scope

This document covers the authorization process for independent laboratories to become ADA Security Test Laboratories (ASTL) and the capabilities required for an organization to do so. The process outlined in this document describes the requirements for ASTLs seeking authorization in the ADA Certification scheme.

The ADA is focused on protecting users by preventing threats from reaching their devices and improving app quality across the ecosystem. The ADA protects users of mobile and web applications, through industry recognized security standards, validation guidance and a certification scheme which scales with risk. ADA requires that ASTL assess applications in accordance with its requirements. Any violations or activities that are not in line with the expectations may result in the revocation of the lab's authorization.

Document Maintenance

The ADA Certification Scheme documentation was created and developed by the ADA, composed of representatives from 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 (ADA)

Certification Body (CB)

ADA Security Test Laboratories (ASTL)

References

ADA Certification Scheme Overview

ADA Evaluation Methodology

ADA Certification Roles

The ADA Certification Scheme involves a number of actors that perform a variety of roles in support of the scheme.

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/IEC 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/IEC 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.
ISO/IEC 17025 Accreditation Body	The accreditation body responsible for conducting ISO/IEC 17025 audits and granting ISO/IEC 17025 certificates to ASTLs, based on requirements laid out by ISO with additional guidance provided by the ADA. This body ensures compliance with ISO/IEC 17025 standards through approved auditors and validates the competence of ASTLs. This is typically an ILAC/Global Accreditation Cooperation Incorporated member that is recognized as having competence to carry out ISO/IEC 17025 test laboratory audits.
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.

ADA Security Test Laboratory (ASTL) Authorization

The ASTLs are required to be authorized before they are able to perform evaluations and submit results to be certified. This process ensures that the ASTLs meet acceptable standards and that the results can be considered trustworthy. The following sections specify the expectations for an authorized ASTL.

ASTL Security Objectives

ASTLs are responsible for ensuring their assets are protected from the risks to which they are exposed. It is this protection that provides assurance to the Developer and other industry stakeholders. A range of security objectives shall be addressed but higher levels of assurance are needed depending on the asset classification.

The intent is to ensure that Authorization of an ASTL under the ADA Certification Scheme means that ASTLs have and maintain the ability to perform meaningful, comprehensible, repeatable, and complete test evaluations of applications. ASTLs must maintain the confidentiality and integrity of their assets and must ensure they attain and maintain the standards of performance described in this document.

ASTL Assets

The main assets of the ASTL that need to be protected, guaranteed and held are:

- Competence of the Laboratory personnel
- Understanding of the threat landscape and threat actor techniques, tactics, and procedures
- Working procedures and guidelines for the Laboratory
- Equipment and tools available to, and used by, the Laboratory
- Confidentiality, integrity and availability of security relevant information from Developers

ASTL Threats

Threats related to the security of the ASTL assets and to which they are exposed include:

- The Laboratory personnel are not sufficiently competent
- The Laboratory lacks understanding of threat landscape and threat actor techniques, tactics, and procedures
- The Laboratory lacks suitable working procedures and guidelines
- The Laboratory lacks suitable equipment and tools
- The Laboratory lacks suitable security mechanisms to protect the confidentiality, integrity and availability of security relevant information from Developers
- The Laboratory is not independent from the Developer, creating a conflict of interest

ASTL Requirements

ASTL Evaluator/Evaluation Team Competency

- The Lab's organizational chart must clearly show the functions and lines of authority for staff within the application's organization and the relationship, if any, between the ADA security assessment functions and other activities of the applicant's organization.
- The Lab shall have different roles to manage, perform or verify the assessments including:

    - Engagement Partner: The partner or other person in the ASTL organization who has the authority to bind the ASTL with respect to the performance of an ADA engagement, who is responsible for the ADA engagement and its performance, and for the assessment report and, as applicable, the Evaluation Reports (including the conclusion for each report) that is issued on behalf of the ASTL and who, when required, has the appropriate authority from a professional, legal, or regulatory body. For purposes of this definition, a partner may include an employee with this authority who has not assumed the risks and benefits of ownership. The ASTL may use different individuals and titles to refer to individuals with authority to bind and to manage the engagement.
    - Engagement Quality Control Reviewer: A partner, other person in the ASTL organization, suitably qualified external person, or team made up of such individuals, none of whom is part of the engagement team, with sufficient and appropriate experience and authority to objectively evaluate the significant judgments that the engagement team made and the conclusions it reached in formulating the Evaluation Reports (including the conclusion for each report).
    - Engagement Team: All partners and staff performing the ADA engagement and any individuals engaged by the ASTL. This excludes individuals within the developer's organization who provide direct assistance on an ADA engagement.
- The ASTL shall maintain impartiality from the Developer. An ASTL's independence is compromised if it:
    - Makes investment decisions on behalf of a developer or otherwise has discretionary authority over a developer's assets
    - Executes a transaction to buy or sell a developer's asset
    - Has custody of assets of the developer, such as taking temporary ownership of a developer's assets.
- Any information received about the Developer from sources other than the Developer (e.g. investigations, findings related to potential security incidents or breaches) shall be confidential between the Developer and the ASTL. The source of this information shall not be shared with the Developer unless agreed by the source.
- The ASTL shall follow all decision rules outlined in the ADA profile test specs (and associated materials) for assigning "pass / fail/inconclusive' verdict.
- The expectation is that the Developer provides a production version of their application. If a production version does not yet exist, the Developer may provide a close to final beta/release candidate. The ASTL is responsible for ensuring that the tested version or environment is identical to the one used in production.
- The application fulfills all the requirements, the ASTL will furnish the appropriate Evaluation Reports.

ASTL Authorization Process

The process for becoming an ASTL includes several steps. While a fully authorized ASTL must be ISO/IEC 17025 accredited to ADA program requirements, this can be a lengthy process. To accommodate this

timeframe, there are provisional stages of authorization that allows an ASTL to start work while still meeting the high requirements for the ADA Certification program.

The three levels of authorization are:

- Provisional 1 ASTL - a Lab that has not yet completed their first three evaluations and is under direct oversight by the CB. (Provisional 1 status is per application type, so completion of a web application evaluation does not mean the Laboratory can perform a mobile application evaluation without oversight).
- Provisional 2 ASTL - a Lab that has completed the oversight evaluation and was considered acceptable by the CB, but is still waiting for the ISO/IEC 17025 accreditation to be completed.
- Authorized ASTL - a Lab that has both completed oversight evaluations and is ISO/IEC 17025 accredited.

Steps for Authorization

Step 1 - Petition to become an ASTL

Contact the CB to become an ASTL. Work with the CB to understand the requirements to become authorized.

Step 2 - Begin the ISO/IEC 17025 Accreditation Process

A prospective ASTL contacts A2LA in pursuit of attaining ISO/IEC 17025 accreditation. The scope of accreditation needs to be specific to the ADA scheme. The expectation is that the ASTL will obtain the ISO/IEC 17025 accreditation within a year of applying.

Once A2LA has deemed the Laboratory's application, TrustCB will grant Provisional 1 ASTL status and the Laboratory can proceed to Step 3 - Trial Evaluation with CB Oversight..

Step 3 - Trial Evaluation with CB Oversight

A prospective ASTL must demonstrate its technical competence at conducting ADA evaluations by successfully passing a trial evaluation with CB oversight.

1. **Mock Evaluation** - A prospective ASTL conducts a mock ADA AL2 evaluation using vulnerable sample apps provided by the CB, such as WebGoat (for the ADA web profile) and DVIA (for the ADA mobile profile), or other similarly known vulnerable apps designated by the CB. The lab then submits their evaluation results and supporting evidence to the CB for review. The CB may conclude that the prospective ASTL has:
    a. Successfully completed the mock ADA evaluation, and therefore can proceed to an actual developer evaluation with CB oversight.
    b. Failed the mock ADA evaluation, and therefore the ASTL is rejected

    Note: a prospective ASTL that has already demonstrated technical competence under an equivalent program (i.e., the appdefensealliance.dev's MASA program, relevant to the ADA's mobile standard, or CASA program, relevant to the ADA's web standard) may supply evidence of this fact and bypass this step.

2. **Trial Evaluation with CB Oversight** - Upon passing the Mock Evaluation, the prospective ASTL may conduct actual developer evaluations but with strict CB Oversight.

   Strict CB Oversight means that instead of (just) submitting evaluation reports (as described in the ADA Evaluation Methodology doc), the prospective ASTL must share with the CB all testing results and evidence used in the evaluation and demonstrate that:
   a. Testing scope was determined appropriately
   b. Each requirement was tested
   c. Each requirement decision was correct
   d. Evaluation reports were completed properly
   e. All relevant testing processes and procedures were followed correctly

   Trial evaluation customer engagements must be done using the AL2 level, with the rationale that an ASTL that is capable of conducting AL2 evaluations will be capable of performing evaluations at lower ALs whereas the converse does not hold.

Trial Evaluation process responsibilities of the CB:

1. Evaluate the technical proficiency of each laboratory to ensure that they are competent to perform specific types of testing.
2. Reviewing the lab's quality management system, assessing its personnel qualifications and training, and observing its testing procedures and methods.
3. The CB may also review the laboratory's equipment and facilities to ensure that they are suitable for the type of testing being performed.
4. Decide whether or not a prospective ASTL that completes a mock ADA evaluation against a vulnerable sample app may proceed to a Trial Customer Engagement
5. Decide whether or not a prospective ASTL that completes a Trial Evaluation has:
   a. Passed the Trial Evaluation process and can considered Provisional 2 ASTL
   b. Requires Additional Trial Customer Engagements before a passing/failing outcome can be determined
   c. Or failed the Trial Evaluation process and is therefore rejected as an ASTL

Step 4 - Completion of the ISO/IEC 17025 Audit

Once the Lab successfully completes the accreditation process, they will provide this credential to the CB. Accreditation in conjunction with successful completion of the trial evaluation will result in the provisional ASTL becoming a fully authorized ASTL.

Note: All steps must be completed to be an authorized ASTL, so achieving ISO/IEC 17025 accreditation without successfully completing the trial evaluation does not automatically move the Laboratory to authorized status.

Maintenance of the Authorization

The authorization provided to an ASTL is not perpetual. ASTLs must operate in accordance with the obligations under ISO/IEC 17025 and must renew their accreditation to keep it current at all times. ASTLs

must inform the ADA CB if their accreditation is revoked for any reason. The ADA CB will revoke authorization from Laboratories that no longer have accreditation.

While audits are typically conducted on a regular schedule, special audits may be initiated outside of this schedule in response to specific circumstances, such as disputes or significant non-conformities identified through the dispute resolution process.

As part of maintaining ISO/IEC 17025 accreditation and ASTL status, ASTL shall conduct intercomparison exercises. To support this, the ADA CB may request ASTLs to conduct an evaluation of a designated app on an annual basis. These evaluations, conducted as part of the intercomparison process, allow ADA to ensure consistency in testing methodologies and results across different labs.

ISO/IEC 17025 Program Specific Requirements

Additional specific requirements for this program are described below. The numbering system for each section corresponds with the major sections of ISO/IEC 17025. If a section is not listed below, there are no program specific requirements beyond what is already stated in ISO/IEC 17025.

Section	**Reference**
4.1.3	If a Developer uses their internal testing Laboratory (one that meets specified lab requirements under ADA and are an authorized assessor), the Laboratory shall have policy and procedures that protect the impartiality of the Laboratory to test or otherwise evaluate apps manufactured by the Laboratory's parent organization, and if applicable, other developers without regard to the impact of the test results on the parent organizations' business interests.
4.1.4	The Laboratory shall maintain independence from the developer and developer's assets.
4.2.1	Unless required by law or contractual commitments, information the Laboratory intends to place in the public domain (i.e., the evaluation reports) requires the express consent of the developer or affiliated authorizing parties.
5.2	Each ADA engagement shall have a designated Engagement Partner and Engagement Team (see roles below)
6.2.2	The CB is responsible to ensure the competence based on other certificates or even the experience of specific persons conducting the evaluations. For the Engagement Team, those performing the assessment must have one of the following certifications for Web App and Cloud Config Profiles: ● Certified Mobile and Web Application Penetration Tester (CMWAPT) ● Offensive Security ○ Offensive Security Web Expert (OSWE) ○ Offensive Security Certified Professional (OSCP)

Section	Reference
	● Global Information Assurance Certification (GIAC) ○ Penetration Tester (GPEN) ○ Certified Web Application Defender (GWEB) ○ Web Application Penetration Tester (GWAPT) ● eWPTX For the Engagement Team, must have one of the following for Mobile App Profile (or be under the supervision of someone with the following): ● Global Information Assurance Certification (GIAC) Mobile Device Security Analyst (GMOB) ● Certified Mobile Security Engineer (CMSE) ● INE Mobile Application Penetration Tester (eMAPT) ● TCM-SEC Mobile Application Penetration Testing For the Engagement Quality Control reviewer: ● Academic training: EQF Level >= 4 ● Complementary training: Knowledge of the technology associated with the Evaluation of Cloud Applications or Android Mobile Applications.
6.2.6	*(17025 text) The laboratory shall authorize personnel to perform specific laboratory activities, including but not limited to, the following:* (d) Dispute management (with process defined in Section 7.9.1 below) (e) Remediation guidance
6.3.2	The lab shall document requirements and conditions necessary for performing lab activities including any permanent and temporarily instantiated virtual environments used for the purposes of performing an assessment or other engagement related procedures.
6.4.1	In the case of ADA mobile evaluations against Android (or Quest) apps, the lab shall have the capability to test applications on a rooted Android mobile (or Quest) device that uses the latest OS version made publicly available.
6.4.1	Some specific tooling (e.g., open source or commercially available application vulnerability scanning software) must meet standards defined by ADA Policies and Procedures.
6.4.3	Where possible, the lab should test the public version of the application from the App Store (specific to mobile apps) to ensure chain of custody.
6.6.2.c	A laboratory is prohibited from relying on an external service provider, in part or in whole, to perform laboratory activities, where such an external service provider is not ILAC/Global Accreditation Cooperation Incorporated signatory Accreditation Body accredited as an authorized assessor, subject to the requirements of this document.
7.2.2.4.b	Specifies what types of records the ASTL retains and the assurance level

Section	Reference
7.5.1	Additional records to be maintained shall include: ● Metadata related to the application in scope for assessment (e.g., application build, unique project identifiers, application environment configurations, etc.) ● Assessment type (e.g., Self-initiated, Framework User) ● Assessment scoping documentation, including: ○ ADA certification type and tier ○ Developer provided security certifications ○ Agreed upon procedures ● Assessment environment (e.g., systems, scripts, tooling) configuration ● All documentation produced in the course of performing the assessment, including assessment procedure inputs and outputs ● Any other documentation as required by the App Defense Alliance Policies and Procedures A Lab should maintain the documentation for a minimum of 2 years after the expiration of the certificate
7.8.2.1	Evaluation Reports shall include: 1. Specifications which were self assessed and not validated by the lab. 2. Specifications which were not evaluated 3. Pass/Fail/Inconclusive verdict for each requirement 4. (For Failed requirements) remediation recommendations specialized to the application 5. Statement of conformity with these requirements
7.8.3.1.e	ADA validation reports, with template provided in ADA Policies & Procedures
7.9.1	The ASTL will be responsible to address the dispute and either update the validation report with ADA CB, or inform ADA CB via email that the dispute has been resolved

The following requirements were omitted as they are not applicable relevant to mobile/web testing.

Not applicable ISO/IEC 17025 Requirements
6.4.5, 6.4.6, 6.4.7, 6.4.8, 6.4.11, 6.4.12, 6.4.13 e
6.5.1, 6.5.2, 6.5.3

7.2.1.4, 7.2.1.6, 7.2.1.7
7.2.2.1, 7.2.2.2, 7.2.2.3
7.3.1, 7.3.2, 7.3.3
7.6.1, 7.6.2, 7.6.3
7.7.1 d,e,f,g,h, 7.7.2
7.8.1.3
7.8.2.1 c, k, l, m, n, o, p
7.8.2.2
7.8.4.1, 7.8.4.2, 7.8.4.3
7.8.6.1
7.8.5
8.1.3

Annex

Document History

Date	**Version**	**Changes**
October 1, 2024	v1.0	First Version

March 24, 2025	v1.1	- Corrected use of “certification” vs “accreditation” and ISO/IEC throughout
		- Detailed updates to the ASTL Authorization process
		  - Step 2 - A2LA must deem the lab’s application complete to proceed
		  - Step 3.1 - Mock Evaluation - Labs that have demonstrated proficiency under a

		predecessor program can bypass this step - Maintenance of the Authorization - updated this section for clarity - ISO/IEC 17025 Program Specific Terms - significant updates to the required qualifications for the engagement team