Australian Government

Digital Transformation Agency

Technical Integration Testing Requirements

Trusted Digital Identity Framework
August 2018, version 1.0

dta

Digital Transformation Agency

Licence

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (http://www.itsanhonour.gov.au)

Conventions

The key words "**MUST**", "**MUST NOT**", "**SHOULD**", "**SHOULD NOT**", and "**MAY**" in this document are to be interpreted as described in the current version of the *Trusted Digital Identity Framework: Overview and Glossary*.

Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you have difficulties accessing this document or have questions or comments regarding this document please email the Director, Trusted Digital Identity Framework at identity@dta.gov.au.

Document Management

The Trust Framework Accreditation Authority has reviewed and endorsed this document for release.

Change log

Version	Date	Author	Description of the changes
0.001	30 Jan 18	CEJ	Initial version
0.002	31 Jan 18	CEJ	Transfer to New Template Include Risk-Based Testing, Defect Management
0.003	13 Feb 18	CEJ	Update after Technical Integration review After review of ISPT
0.004	12 Mar 18	CEJ	Final Review
0.01	19 Mar 18	CEJ	Draft Release
0.02	20 Mar 18	CEJ	After review by DTA, minor changes
0.03	Jul 2018	GJF	Updates based on stakeholder feedback
1.0	Aug 2018		Approved for release by the TFAA

Contents

List of Tables

1 Introduction

The Digital Transformation Agency (DTA), in collaboration with other government agencies and key private sector bodies, is leading the development of a national federated identity 'eco-system' (the 'identity federation'). Implementation and operation of the identity federation is underpinned by the Trusted Digital Identity Framework (TDIF). This document should be read in conjunction with the *TDIF: Overview and Glossary*, which provides a high-level overview of the TDIF including its scope and objectives and the definition of key terms.

This document defines the testing processes that are implemented to run an effective technical integration-testing[1] program and demonstrate conformance to the TDIF requirements. Technical Integration Testing Requirements includes:

- Testing against the integration requirements included in the Trust Framework Technical Standards and Profiles[2],
- System Testing against the required functionality specified in the TDIF, and
- Security Testing against the testable requirements specified in the TDIF Protective Security documents[3].

This document defines what is to be included in a testing program and what documented information is required to achieve and retain TDIF accreditation. It does not define how testing is to be undertaken nor what tools will be used or how the records of testing are retained.

The Technical Integration Testing Requirements are implemented for an Applicant's identity service and maintenance of an Accredited Provider's identity system; it is applied throughout the life of a system from the initial development and continues to be applicable through all maintenance and support activities.

- This document defines the technical integration testing requirements of the TDIF Accreditation Process[4].

[1] Integration testing is a systematic, incremental approach to the assembly of a system, in this case the identity federation. The focus is on demonstrating that the components of a system interface correctly and fulfil the functions specified for them.

[2] Includes the Attribute Profile, SAML Profile and OIDC Profile documents.

[3] Includes the Protective Security Requirements and Protective Security Reviews documents

[4] See the *TDIF: Accreditation Process* for further information on the TDIF accreditation process.

The Technical Integration Testing Requirements are applicable to both the development and accreditation of a new system and the accreditation of an existing system.

The Technical Integration Testing Requirements are applicable from initial Accreditation and transition to a production system through in-service sustainment and maintenance, covering:

- **Initial accreditation** – technical integration testing of an Applicant's system to demonstrate compliance to the requirements of this document.
- **Ongoing accreditation obligations** – maintenance and modification to an Accredited Provider's identity service after it has achieved Trust Framework Accreditation and transitioned to the production environment for operational use, including:
    - **Major Changes** – the development of new or changed functionality which implements substantial changes to the system, infrastructure or requirements.
    - **Enhancement** – the development of new or changed functionality to an existing system without substantially changing the system, including minor upgrades.
    - **Defect** – correction to existing system that was in place to deliver a defined and approved functionality where the system does not meet that functionality and requires modification.

The intended audience for this document includes:

- Accredited Providers.
- Applicants (including Identity Service Providers [IdPs], Credential Service Providers [CSPs], Attribute Providers [AP] and Identity Exchanges [IdX]).
- Relying Parties.
- Trust Framework Accreditation Authority.

2 Requirements

The Applicant **MUST** provide the Accreditation Authority with sufficient documentation (test plans, test reports, etc) to demonstrate the Applicant has achieved the Technical Integration Testing Requirements.

2.1 Design Verification

Design Verification[5] is intended to make sure that no technical integration requirements are missed in the design.

The Applicant or Accredited Provider takes the design inputs, specifications, government and industry regulations and verifies that each requirement in the inputs is accounted for in the outputs. This **MUST** include:

- Requirements Traceability Matrix (RTM) against all mandatory and the selected optional requirements.
- Method of Validation[6] (record of validation of a setting/control or test case for execution during the Testing Phase).

Note:
The RTM is a Test Artefact that is created during Design Verification and updated throughout the Test Management Process.

2.2 The Fundamental Test Process

The Fundamental Test Process is a logical sequence of activities that governs the actions undertaken throughout the testing lifecycle and is considered to comprise of five basic activities:

- Planning (including Test Risk Priority).
- Specification (including the Test Environment and Test Entry).
- Execution.
- Recording.

[5] The term Verification is defined in this document to be specific to the context of Testing.
[6] The term Validation is defined in this document to be specific to the context of Testing.

- Checking for Test Completion.

The main goal of the Fundamental Test Process is to define the minimum testing activities in order to achieve the outcomes and goals of the respective tests focus.

Testing activities **MUST** be carried out to:

- verify and validate that all applicable Trust Framework requirements have been addressed;
- demonstrate a system is compliant with all applicable Trust Framework requirements;
- develop an effective test suite that can be maintained throughout the life of a system to provide effective regression testing; and
- uncover as many issues as possible and contribute to the deployment into the production environment of a robust secure system.

2.2.1 Test Management Processes

Test Management Processes define the planned activities for the management of testing by an Applicant or Accredited Provider. Table 1: Test Management Processes describes the individual processes.

Table 1: Test Management Processes

Process	Details	Outcome
Test Planning	Outlines the approach for testing planned for Accreditation Application and maintenance of an Accredited system	Test Plan(s)
Risk-Based Testing	Identifying requirement risk and assign a Test Priority to ensure optimum testing	Test Risk Priority
Test Environment	Defines the Test Environments consumed, and the testing undertaken in each environment known.	Test Environments known and documented
Test Entry	Controls the entry into testing	Test Entry Assessment

Process	Details	Outcome
Test Monitoring and Control	Ensures Test Sets are executed in accordance with Test Implementation During test execution monitors through Test Status Reporting	Progress against Test Plan monitored Deviation from Test Plan and actions to control New or changed Risks identified New or changed Test Cases identified Test Incident Reporting and Defect Management
Test Completion	At the completion of Test Execution a report is raised. Formal Exit from Testing	Test Exit Assessment Test Completion Report

2.2.1.1 Test Planning

A Test Plan **MUST** be developed by the Applicant or Accredited Provider defining the approach for testing planned for an Applicant's system and maintenance of an Accredited System.

There **MAY** be a single Test Plan for the Accreditation and maintenance of an Accredited system, or multiple Test Plans, for each individual phase.

Table 2: Test Plan Contents, specifies the Test Plan mandatory content that **MUST** be included.

Table 2: Test Plan Contents

Process	Details
Scope	Describes the coverage, including: • Inclusions, • Exclusions, and • Limitations
References	List of Test References, including: • Trusted Framework Requirements • Design
Context of Testing	Identifies the context for which the Test Plan is being written

Process	Details
Test Scope	A summary of the items under Test, **SHOULD** include: • Features • Attributes • Interfaces • Functions
Assumptions, Limitations and Dependencies	Describes the assumptions, limitations and dependencies relevant to the Test Plan. For example, this **MAY** include: • Simulation of messages received and sent by either an Identity Provider or Exchange Provider. • Completion of Design Verification prior to Test Entry.
Risk	This **MAY** include a reference to the Risk Register or Risk Management Plan and specify how the Test Cases are rated for Test Priority based upon risk. This **MUST** comply with the Risk-Based Testing approach required for Trusted Framework Accreditation.
Test Approach	Describes the approach for testing each of the Minimum Test Coverage areas, including any automated testing.
Test Incident and Defect Management	Describes how any test incident (where the actual execution result does not match the expected result), the analysis of a test incident and the raising and management of any incident considered to be a defect.
Test Artefacts	Identifies all the Test Artefacts that are produced as a result of the testing activity. This **MUST** include: • Test Plan • Test Specification • Test Cases • Test Data • Test Entry Criteria • Test Execution Log • Test Incident Register • Defect Register • Test Completion Report
Test Entry	Describes the Test Entry Criteria Assessment undertaken for entry into testing.
Test Exit	Describes the Test Exit Criteria Assessment undertaken, including execution coverage and defect limits considered the minimum conditions under which the testing is considered complete.

Process	Details
Test Data	Describes the Test Data required for each phase of testing, the source and any security requirements, including as appropriate: • Anonymisation of any production data where Personal Identifying Data may be compromised. • Simulated Data (where the interfacing system is not available for testing).
Test Environment	Specifies the required test environment properties.
Test Resources	Specifies the resources (equipment, applications, tools) required for testing activities.
Retesting and Regression	Specifies the conditions under which retesting and regression testing is performed.
Suspension and Resumption	Specifies the criteria for suspension of testing and the testing activities that **MAY** have to be repeated upon resumption.
Roles and Responsibilities	Specifies the testing roles and the responsibilities assigned.

2.2.1.2 Risk-Based Testing

The categorisation of test risk **MUST** comply with the Risk Management Process defined in the *TDIF: Risk Management Requirements* document.

The Applicant or Accredited Provider **MUST** assess the risk and assign a risk rating to all testable requirements, this will give the priority for all Test Cases derived from a requirement.

The Test Case Priority will define those Test Cases that **MUST** be executed. This is the minimum test execution coverage, compliance with this is the condition under which the testing is considered complete. The priorities are as follows:

- Priority 1 (Critical) – Indicates critical functionality that could lead to a complete system failure, or present a security threat, in the event that it is untested e.g. a test that verifies a firewall is operational.
- Priority 2 (High) – Indicates functionality that could lead to complete failure of a sub-system, or a piece of important functionality, in the event that it is untested e.g. a test that verifies that an application can be launched and accessed by a user.

- Priority 3 (Medium) – Indicates functionality that may cause incomplete, inconsistent, or incorrect results in the event that it is untested e.g. a test that verifies the automatic start or update of an isolated component.
- Priority 4 (Low) – A test that should be executed after all other higher priority tests have been run. Indicates functionality that is desirable but not crucial to the solution e.g. test that verifies some text spelling or punctuation.

Table 3: Test Case Priority and Minimum Execution Coverage defines the rating and priority that **MUST** be complied with.

Table 3: Test Case Priority and Minimum Execution Coverage

Risk Rating	Test Priority	Minimum Execution Coverage
Extreme	1 (Critical)	100%
High	2 (High)	100%
Moderate	3 (Medium)	90%
Low	4 (Low)	80%

2.2.1.3 Test Environment

The Test Environment requirements and the set-up process **MUST** be defined by the Applicant or Accredited Provider. Table 4**:** Test Environments define the Test Environments that **MAY** be used and the types of testing executed in each.

Table 4: Test Environments

Environment	Connectivity	Testing Executed	Data	When
Test Environment (MAY also be known as Systems Integration Test Environment)	Application not interfaced with CSP, AP or IdP or IdX (as appropriate)	• System Testing • Technical Integration Testing • Security Control Testing (to ensure settings work as required)	• Simulated • Test Data, or • Anonymised Copy of Production Data	For testing confined to internal testing: • Prior to Accreditation • Post Accreditation for Change Requests

Environment	Connectivity	Testing Executed	Data	When
	Application interfaced with CSP, AP or IdP or IdX Test Environment (as appropriate)	• System Testing • Technical Integration • Event Management • Security Control Settings (to ensure they work as required)	• Test Data, or • Anonymised Copy of Production Data	For end-to-end testing: • Prior to Accreditation • Post Accreditation for Change Requests
Pre-Prod	Application interfaced with CSP, AP or IdP or IdX Test or Pre-Prod Environment (as appropriate)	• Change Testing • Operational Readiness Testing	• Anonymised Copy of Production Data	For confirmation of Operational Readiness Testing: • Prior to Accreditation • Post Accreditation for Change Requests
Production	Application interfaced with CSP, AP or IdP or IdX Production Environment (as appropriate)	• Service Operation Testing • Technical Integration Testing • Security Control Testing (to ensure they work as required) • Pen Testing • Health Check • Business Continuity Disaster Recovery	• Production Data	For Service Operation Testing: • Prior to Accreditation • Post Accreditation

2.2.1.4 Test Entry

Prior to commencement of Test Execution, the Applicant or Accredited Provider **MUST** be satisfied of the following:

- The Test Plan is approved and released
- Design Verification is complete
- All requirements are included in the RTM

- All requirements have a risk rating
- All requirements are covered by one or more Test Cases
- All Test Cases are complete
- All Test Cases have a Priority assigned based upon the risk rating
- All test resources are identified and available

A documented record of the Test Entry Assessment **MUST** be retained, which **MAY** be either a minute of a meeting or a Test Entry Assessment Report.

2.2.1.5 Test Monitoring and Control

The Test Monitoring and Control Process is essentially a management activity and determines whether the testing activities are in accordance with the Test Plan, schedule and planned outcomes. It will initiate control actions as necessary and identify updates to Test Artefacts.

This **SHOULD** include:

- Test Status analysis and reporting
- Test Entry assessment
- Progress against Test Plan monitored
- Deviation from Test Plan and actions to control
- New or changed Risks identified
- New or changed Test Cases identified
- Test Incident Reporting and Defect Management
- Preparation for Test Completion

2.2.1.6 Test Completion

Test Completion **MUST** include both the:

1. Test Completion Report, and
2. Test Exit Assessment.

Test completion is undertaken when testing activities are complete. The Test Completion Criteria is:

- The pass rate for all Test Cases exceeds 95.0%,
- All Test Incidents and Defects uncovered during testing have been documented,

- There are no Open Severity 1 Defects,
- There are no Open Severity 2 Defects,
- There are no more than ten (10) open Severity 3 Defects unless a formally accepted remediation plan is in place,
- There are no more than twenty (20) open Severity 4 Defects unless a formally accepted remediation plan is in place.

2.2.1.6.1 Test Completion Report

The Test Completion Report provides evidence that testing outcomes are within planned tolerances and supports the Test Exit Assessment. Test Completion Report **MUST** include:

- Demonstration testing has been executed in accordance with the approved Test Plan;
- Test Case execution coverage has been completed in accordance with Table 3: Test Case Priority and Minimum Execution Coverage
- All Test Execution results are recorded; and
- Test Completion Criteria has been met, where the criteria have not been met a risk-assessment must be included for approval to deviate and exit testing.

2.2.1.6.2 Test Exit Assessment

The Test Exit Assessment is the final Test Process phase and is designed to ensure that all testing activities are complete.

The Test Exit Assessment **SHOULD** be undertaken as a formal meeting with applicable parties represented[7]. Each of the decisions for the specific criteria are recorded and minutes of the meeting taken to record the outcome.

The Test Exit Assessment **MUST** include:

- Testing has been performed in a manner consistent with the relevant Test Plan,
- The Test Completion Report has been approved,
- All deviations from the Test Completion Criteria have been approved, and
- Conduct analysis to assess whether additional Test Execution effort is required to demonstrate that the System is fit for purpose.

[7] NB: The Accreditation Authority **SHOULD** be invited and **MAY** participate in Integration Test Exit Assessments.

2.2.2 Testing Process

The Testing Process comprises activities for the analysis, design and development of test specifications and test cases. It also covers the records of test execution results, incidents and defects. **Table 5:** Testing Processes describes the individual processes.

Table 5: Testing Processes

Process	Details	Outcome
Test Analysis and Design	Identifies the features to be tested and the Test Conditions. Updated RTM for requirements confirmed through testing.	Test Specification Requirements Traceability Matrix
Test Case Development	Test cases are designed and written based on the requirements. Updated RTM with Test Case against requirements.	Test Cases Requirements Traceability Matrix
Test Implementation	Plan the test execution cycles comprising of the Test Cases in one or more test set.	Test Sets
Test Execution	The Test Execution Log defines	Test Execution Log
Test Incident Reporting		Test Incident Log
Defect Management		Test Defect Log

2.2.2.1 Test Analysis and Design

The purpose of the Test Analysis and Design activities is to analyse the requirements and identify Test Cases that will be executed during Test Execution.

As a result of this activity the:

- requirements to be tested are identified,
- Test Conditions are derived,
- Test Data is identified,
- Test Cases are derived, and
- Test Case Priority derived.

The Test Design Specification **MAY** be either in a Test Tool or a Test Case Specification document.

The RTM **MUST** be updated with the Test Case detailed for all requirements identified as testable.

2.2.2.2 Test Case Development

Test Cases detailing the specific steps and expected results are written to validate that all requirements have been met and that the system functions as specified in the design documentation.

Each Test Condition for a requirement **MUST** have a Test Case.

Test Cases **MAY** provide evidence of conformance to more than one requirement or Test Condition. Where this occurs the Test Priority will be the priority derived from the highest Risk Rating.

All developed Test Cases **MUST** be peer reviewed prior to Test Execution.

2.2.2.3 Test Implementation

Test Implementation is the set of activities where Test Cases are transitioned from development to execution readiness through the creation of Test Sets and orders their Test Execution. The major tasks involve:

- Create test scripts and data.
- Verify the test environment.

Test Implementation **SHOULD** be completed prior to the commencement of the Test Execution.

2.2.2.4 Test Execution

During Test Execution Test Cases developed during the previous phases are executed and the expected and actual results compared. During this phase Defects are likely to be identified, resolved, retested, and related areas Regression Tested.

During manual Test Execution the tester running the test **MUST** record and retain the actual results, in real time, as evidence of execution.

The output from automatic Test Execution **MUST** be recorded in the Test Execution Log and retained.

- Test Case identification reference,
- Test Name,
- Traceability to the requirement(s) in the RTM
- Execution Status (Pass/Fail)
- Execution Date/Time,
- The Tester who ran the Test Case.

Note:
Where a Test Tool is used to record execution the Test Execution Log MAY be extracted as a report.

To supplement the scripted Test Cases, and endeavour to increase test coverage, Exploratory Testing **MAY** be conducted in addition to the planned Test Cases.

If a test step does not produce the expected result (the actual result does not match the expected result), a Test Incident Report (TIR) **SHOULD** be raised.

At the completion of executing a Test Case the result (Pass or Fail) **MUST** be recorded.

2.2.2.5 Test Incident Reporting

Each TIR **SHOULD** contain the following minimum information:

- Source identification (Test Case, Test Script, Step Number).
- Description.
- Severity (initially set by the Tester using the definitions from Defect Management)
- Action Taken (narrative of actions during any analysis of TIR).
- Resolution.
- Defect ID (if the TIR results in the raising of a Defect or Enhancement).
- Status (Open or Closed).

Where the actual result does not match the expected result during the execution of a Test Case it is not assumed that the Test Incident Report is a Defect. Each TIR will be assessed to determine the root cause and resolution.

All TIRs **MUST** be resolved and the following assigned as the resolution before a TIR can be closed:

- New Defect

  A New Defect is raised in accordance with Defect Management, the Defect id is recorded and the TIR closed.
- Existing Defect

  The Defect id is recorded and the TIR closed.
- Error in Test Case

  The Test Case is corrected and the TIR closed.
- Error in Test Execution

  The Test Case is re-executed and the TIR closed

2.2.2.6 Defect Management

All defects raised **MUST** be managed from identification through resolution and successful re-testing before they can be closed.

All defects **MUST** be assigned a severity based upon the impact of the defect. There are 4 Defect Severities, as follows:

- Severity 1 (Critical) – Critical errors that render a system completely unusable, or affect critical data, and there is no workaround.
- Severity 2 (High) – Major errors that render a system unusable, or affect critical data, but a suitable workaround can be implemented.
- Severity 3 (Medium) – Moderate errors that result in incomplete, inconsistent or incorrect results, where a workaround can be easily implemented to yield the desired result.
- Severity 4 (Low) – Minor / Cosmetic issues that result in undesirable outcomes but do not affect functionality or result in incorrect results.

2.3 Minimum Test Coverage

The minimum required testing for an Applicant's system and maintenance of an Accredited System **MUST** include the requirements for testing included in the following paragraphs.

All Test Cases **MUST** have a Test Risk Priority in accordance with the requirements of Risk-Based Testing.

2.3.1 Technical Integration Testing

The focus for testing is to demonstrate conformance to the Trust Framework Technical Standards and Profiles[8].

The minimum Technical Integration Testing required for Accreditation and maintenance of an Accredited System **MUST** include the testable requirements included in the Trust Framework Technical Standards and Profiles[8].

2.3.2 System Testing

System testing is testing conducted on the complete system being accredited. The focus is to evaluate the system's compliance to the required functionality specified in the TDIF.

The minimum System Testing required for an Applicant's system and maintenance of an Accredited System **MUST** include the testable requirements included in the Trust Framework documents.

2.3.3 Security Testing

New and updated systems require thorough security testing including detailed plans, test inputs and expected results. The focus for security testing is to ensure the Accredited System operates as expected and only as expected.

Security Testing for an Applicant's system and maintenance of an Accredited System **MUST** include the testable requirements included in the Trust Framework Protective and Information Security documents and the security testing requirements detailed in the Service Operations Testing Requirements.

[8] Includes the Attribute Profile, SAML Profile and OIDC Profile documents.

Security Test Cases **MUST** always have a Test Risk Priority of High, the execution of these Test Cases **MUST** be Mandatory.

3 References

The following information sources have been used in developing this document.

1. AS NZS ISO IEC IEEE 29119.1-2015 Software and systems engineering – Software testing – Concepts and definition
2. AS NZS ISO IEC IEEE 29119.2-2015 Software and systems engineering – Software testing – Test processes
3. AS NZS ISO IEC IEEE 29119.3-2015 Software and systems engineering – Software testing – Test documentation
4. ISO IEC IEEE 29119-4-2015 Software and systems engineering – Software testing – Part 4- Test techniques