Australian Government
Digital Transformation Agency

Service Operations 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	15 Feb 18	CEJ	Initial version
0.002	13 Mar 2018	CEJ	Final Review
0.01	19 Mar 2018	CEJ	Draft Release
0.02	20 Mar 2018	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.

Service Operations covers those processes and activities involved in the operation and management of an Accredited Provider's identity system.

Service Operations testing demonstrates conformance of the testable aspects of operating an In-Service (Production) system to the *TDIF: Service Operations Requirements*. Service Operations testing will, as a minimum, include:

- Service Design (Design Coordination, Capacity, Continuity and Security),
- Service Transition (Service Validation[1] and Testing), and
- Service Operations (Event, Application and Technical Management).

This document defines the Service Operations testing requirements of the TDIF Accreditation Process[2].

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.

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

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

2 Service Operation Testing

The Service Operations Testing Requirements are applied during Accreditation and continue to be applicable for the life of an Accredited System. Service Operations Testing **MUST** be undertaken:

- As part of operational readiness testing.
- During sustainment and maintenance of an Accredited System.

Table 1: Service Operation Testing overview describes at a high level the requirements for Service Operation Testing.

Table 1: Service Operation Testing overview

Environment	Connectivity	Testing Executed	Data
Pre-Accreditation	Where the Applicant is a CSP, AP or IdP the Applicant's system is connected to an IdX Test, Pre-Production or Production Environment (prior to transition into service). Where the Applicant is an IdX the Applicant's system in a Test, Pre-Production or Production Environment (prior to transition into service) is connected with a Test CSP, AP or IdP.	• Security Control Testing • Penetration Testing • Health Check • Business Continuity Disaster Recovery	• Test Data, or • Anonymised Copy of Production Data
Post-Accreditation	Accredited Provider System interfaced with IdX, CSP, AP or IdP Production Environment (as appropriate)	• Service Operation Testing • Technical Integration Testing • Security Control Testing • Penetration Testing • Health Check • Business Continuity Disaster Recovery	• Production Data

A Service Operations Test Plan defining the planned approach for testing an Accredited System **MUST** be developed by the Applicant.

The *TDIF: Technical Integration Testing Requirements* provides guidance for Test Planning that **MAY** be followed for the Service Operations Test Plan.

2.1 Pre-Accreditation Operational Readiness Testing

The Service Operations testing requirements are applicable for the testing required for operational readiness and **MUST** be undertaken as series of collaborative tests with the Trust Framework Accreditation Authority to ensure operational readiness of the end-to-end service.

2.2 Post Accreditation Production Operation Testing

After a system is Accredited and has successfully transitioned into service the Accredited Provider is required to maintain Accreditation. Production Service Operation Testing **MUST** be undertaken in order to maintain TDIF Accreditation from year to year.

The *TDIF: Technical Integration Testing Requirements* provides guidance for accreditation maintenance that **SHOULD** be followed for when post accreditation production operation testing is to be undertaken.

2.2.1 Service Operations Testing

Service Operations Testing is applicable through in-service sustainment and maintenance, covering:

- Change Management
- Service Operations Health Testing
- Security Control Testing
- Business Continuity Disaster Recovery Testing

2.2.2 Technical Integration Testing

The *TDIF: Technical Integration Testing Requirements* is applicable through in-service sustainment and maintenance for all changes to the Accredited System.

3 Requirements

3.1 Design Coordination

Design Coordination aims to coordinate all service design activities, processes and resources to ensure the consistent and effective design of changes to an Accredited System. In order to verify all the design inputs are accounted for in the Accredited System design verification[3] activities **MUST** be undertaken by the Applicant.

The Design Verification requirements are defined in the *TDIF: Technical Integration Testing Requirements*.

3.2 Test Management and Testing

The Test Management and Testing Process is defined in the *TDIF: Technical Integration Testing Requirements*.

The test management and testing process **MUST** be applied:

- by an Accredited Provider throughout sustainment of the Accredited System.
- by an Accredited Identity Exchange when on-boarding either a Credential Service Provider, Attribute Provider, Identity Provider or a Relying Party.
- by an Accredited Credential Service Provider, Attribute Provider or Identity Provider when on-boarding to an Accredited Identity Exchange.

3.2.1 Test Plan

The Service Operations Test Plan **MAY** utilise a Change Request Process to manage testing for minor enhancements and defect re-testing.

Major changes **SHOULD** be managed with a change specific Test Plan.

[3] The term Verification is defined in the *TDIF: Overview and Glossary*.

3.3 Test Environment

The Test Environments that **MAY** be used and the types of testing executed in each are defined in the *TDIF: Technical Integration Testing Program*. Applicants that **SHOULD** advise the Accreditation Authority if different test environments are proposed or utilised and provide a statement of equivalency to those defined in the *TDIF: Technical Integration Testing Requirements*.

3.4 Test Data

If change is internal to an Accredited Credential Service Provider, Attribute Provider, Identity Provider or Identity Exchange simulated test data **MAY** be used to validate the change.

If change impacts the interface between an Accredited Credential Service Provider, Attribute Provider, Identity Provider or Identity Exchange then Test Data **MUST** be used to validate the change.

In order to support testing activities a high level of access may be provided to testers which may result in a test environment not having the same security protections as the production environment. Therefore, all production data used in any test environment **MUST** be anonymised[4] prior to being used during testing.

3.5 Change Management

All Changes to an Accredited Provider's identity service **MUST** be managed through a formal Change Management Process that **MUST** include testing of all changes in an environment other than the production environment prior to deployment of the change into production.

Testing of all changes **MUST** conform to the requirements of the *TDIF: Technical Integration Testing Requirements*.

[4] Removing all personally identifiable information from the data sets

3.6 Service Operational Health Testing

Service Operations Testing **MUST** include as a minimum:

- Event management testing to ensure that events are captured and filtered and correlated in accordance with specified requirements.
- Capacity management to ensure that the performances and capacities of the Accredited Provider's identity service meets the agreed targets.

A schedule for the frequency of Service Operation Testing **MUST** be included in the Service Operations Test Plan.

3.7 Security Testing

Security testing utilises vulnerability assessment and penetration testing mechanisms. Security testing **MUST** include the testing of all testable security controls requirements to ensure that the controls are operating as required.

Security testing is undertaken in accordance with the *TDIF: Protective Security Reviews.*

Security testing **MUST** include requirements for regular testing in accordance with the Accredited Provider's Security Risk Management Plan.

A schedule for the frequency of security testing **MUST** be included in the Service Operations Test Plan.

Subsequent to accreditation and after the initial penetration test has been conducted, and any issues resolved, an Accredited Provider **MUST** conduct regular retesting of penetration testing.

3.8 Business Continuity Disaster Recover Testing

Business Continuity Disaster Recovery testing **MUST** be planned and undertaken annually[5], including failover to the disaster recovery site and failback to the production site.

[5] Note – such testing **MUST** include applicable outsourced services that comprise the Applicants system.

4 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
5. ISO_IEC_20000-1-2011_Information_technology_-_Service_management_-_Part_1-_Service_management_system_requirements