TDIF Statement of Claims

Contact Details

Applicant Name:	
ABN:	
Contact Name:	
Contact Email:	
Contact Phone:	

Complexity of System

1. **Which TDIF Role(s) are you seeking accreditation for:**
   - ☐ Identity Service Provider
   - ☐ Credential Service Provider
   - ☐ Attribute Service Provider
   - ☐ Identity Exchange

2. **Are you seeking accreditation for your digital identity service as part of a multi-entity[1] request?**
   - ☐ Yes
   - ☐ No

3. **Would you prefer to be accredited for all roles at once?**
   - ☐ All at once
   - ☐ Sequentially
   - ☐ NA – only one role

[1] **Multi-entity Identity Systems.** Organisations that provide components of an Identity System that work together to perform the functions of one of the TDIF Accredited Roles

4. **Do you want to join the Australian Government's Identity Federation (the Digital Identity system)**

   ☐ Yes

   ☐ No

5. **Where is the ICT infrastructure for your digital identity service located? (state/territory and country for data centre. If cloud-based, please describe)**

6. **Is the digital identity service operational or able to operate with production-like settings?**

Digital Identity Risk Management

7. **How do you manage digital identity risks? (Please provide a statement)**

8. **Has the digital identity service undergone an independent security assessment in the past 12 months? (If yes, please specify Assessor and Assessment Type)**

9. **Has the digital identity service undergone an independent penetration test in the past 12 months?**
   - ☐ Yes
   - ☐ No

10. **Has the digital identity service undergone an independent privacy impact assessment in the past 12 months?**
   - ☐ Yes
   - ☐ No

User Benefit

Identity Service Providers

If you are seeking accreditation as an Identity Service Provider, please answer the following questions.

11. **Which Identity Proofing Levels are you seeking accreditation for? (select all that apply)**
   - ☐ IP1 Plus
   - ☐ IP2
   - ☐ IP2 Plus
   - ☐ IP3
   - ☐ IP4

12. **Which of the following Australian-issued identity document types can be verified using your digital identity service?**
   - ☐ Commencement of Identity documents (CoI)
   - ☐ Photo ID documents
   - ☐ Use in the Community Documents
   - ☐ Linking documents

13. **Which Source Verification service(s) does your identity service provider use to verify EoI Documents as part of Identity Proofing?**
   - ☐ Document Verification Service
   - ☐ Other (please specify)

   - ☐ None (use of Technical Verification or Visual Verification)

14. Does your identity service support an offline channel (e.g. visual verification)?

- ☐ Yes
- ☐ No

15. Does your service support identity lifecycle management (i.e. a reusable identity)?

- ☐ Yes, reusable identity
- ☐ No, one-off verification

16. If your identity service supports IP levels 2 Plus, 3 and 4, which Biometric Matching methods are used by your identity service when performing Biometric Verification?

- ☐ Source Biometric Matching (e.g. using the Facial Verification Service)
- ☐ Technical Biometric Matching (e.g. using an algorithm to compare the photo on the RFID chip with an acquired image)
- ☐ Manual Face Comparison (e.g. using an Assessing Officer to perform biometric matching as part of an in-person transaction)

17. Does your digital identity service support alternative methods to assist people to verify their identity? (e.g. use of trusted referees or attestations[2]) If so, please provide a brief description below.

18. Which of the following user cohorts can verify their identity using your identity service?

- ☐ Individuals whose birth was not registered.
- ☐ Individuals who are homeless or displaced.
- ☐ Undocumented arrivals to Australia.
- ☐ Individuals living in remote areas.
- ☐ Individuals who do not have enough identity documents to meet an IP level (e.g. foreign nationals living in Australia).
- ☐ Individuals who do not have any identity documents but need a digital identity (e.g. foreign national living overseas).
- ☐ Individuals of diverse gender identity.
- ☐ Individuals of diverse sex.
- ☐ Individuals effected by natural disasters.

[2] Further information regarding Alternative Proofing methods can be found in section 3.3 of TDIF 05 Role Requirements

- ☐ Individuals with limited access to identity documents (e.g. individuals who were raised in institutional or foster care).
- ☐ Individuals with limited participation in society.
- ☐ Young people and those over 18 years who are yet to obtain identity documents.

18a. Do you offer your digital identity service as a "white label"[3] service?

- ☐ Yes
- ☐ No
- ☐ No, our service is both an IdP and CSP

Credential Service Providers

If you are seeking accreditation as an Credential Service Provider, please answer the following questions.

19. Which of the following Credential Levels are supported by your digital identity service?

- ☐ CL1
- ☐ CL2
- ☐ CL3

20. Which of the following credential types are supported by your digital identity service?

- ☐ Memorised secret.
- ☐ Look-up secret.
- ☐ Out-of-band device.
- ☐ Single-factor One-Time-Password device.
- ☐ Single-factor cryptographic software.
- ☐ Single-factor cryptographic device.
- ☐ Multi-factor One-Time-Password device.
- ☐ Multi-factor cryptographic software.
- ☐ Multi-factor cryptographic device.

21. Does your identity service support biometric authentication?

- ☐ Yes
- ☐ No

22. Do you offer your digital identity service as a "white label"[3] service?

- ☐ Yes
- ☐ No
- ☐ No, our service is both an IdP and CSP

[3] A white-label product is a product or service produced by one company that other companies rebrand to make it appear as if they had made it.

Attribute Service Providers

If you are seeking accreditation as an Attribute Service Provider, please answer the following questions.

23. Which of the following Attribute Classes are you seeking accreditation for?

- ☐ Authorisation attributes
- ☐ Qualification attributes
- ☐ Entitlement attributes
- ☐ Assumed-Self asserted attributes (e.g. for Tell Us Once services)
- ☐ Platform and ICT infrastructure attributes

Identity Exchanges

If you are seeking accreditation as an Identity Exchange, please answer the following questions.

24. Does your digital identity service support OpenID Connect 1.0 federation protocol?

- ☐ Yes
- ☐ No

25. Does your digital identity service support SAML 2.0 federation protocol?

- ☐ Yes
- ☐ No

26. Does your digital identity service support single sign on, single logout?

- ☐ Yes
- ☐ No

27. Does your digital identity service support a User Dashboard where users can view and manage consent?

- ☐ Yes
- ☐ No

28. Does your digital identity service support Identity Service Provider selection?

- ☐ Yes
- ☐ No

Strategic Value

29. What kind of architecture does your digital identity service operate on?

- ☐ Web-responsive design
- ☐ Mobile Application

30. Which of the following user cohorts have you tested your digital identity service with?

- ☐ Individuals living with a disability.
- ☐ Individuals 65 years in age or older.
- ☐ Individuals who use assistive technologies.
- ☐ Individuals with low literacy.
- ☐ Individuals from culturally and linguistically diverse backgrounds.
- ☐ Individuals who are Aboriginal and/or Torres Strait Islander.
- ☐ Individuals from regional and remote areas.
- ☐ Individuals with older technology and low bandwidth connections.

31. Approximately how many people currently use or interact with your digital identity service?

32. Approximately how many people do you anticipate will use or interact with your digital identity service at least once within the next 12 months?

- ☐ 0 - 50,000 users or transactions
- ☐ 50,001 – 100,000 users or transactions
- ☐ 100,001 – 500,000 users or transactions
- ☐ 500,001 – 1,000,000 users or transactions
- ☐ More than 1 million users or transactions

33. How many online Commonwealth government Relying Party services can be accessed with/though your digital identity service today?

34. **How many online jurisdiction government Relying Party services can be accessed with/through your digital identity service today?**

35. **How many online private sector Relying Party services can be accessed with/through your digital identity service today?**

36. **In the past 12 months have you promoted your digital identity service to a Commonwealth government minister? (Please specify)**

37. **Why are you seeking accreditation?**

- [ ] To participate in new or emerging markets
- [ ] To support government priorities
- [ ] Other (please specify)

Readiness

38. **Do you understand how to read TDIF requirements and applicability indicators?**

- [ ] Yes
- [ ] No

39. **Have you considered all applicable TDIF requirements for your digital identity service?**

- ☐ Yes
- ☐ No

40. **Do you know roughly how many TDIF requirements are applicable for the accreditation you seek?**[4]

41. **Will you be seeking to use prior audit work to satisfy any of the Functional Assessments? (please specify)**

42. **Have you organised Assessors to undertake the necessary Functional Assessments?**

- ☐ Privacy Impact Assessment
- ☐ Privacy Assessment (against TDIF requirements)
- ☐ Security Assessment
- ☐ Penetration Test
- ☐ Accessibility Assessment

43. **Will you be seeking any exemptions against TDIF requirements? (Please specify)**

[4] The *TDIF Accreditation Requirements – template* is available from the Digital Identity website and can be used to filter non-applicable requirements.

a. **Do you have the necessary supporting evidence ready for your exemption request?**

- ☐ Yes
- ☐ No

44. Do you have a dedicated team ready to undertake TDIF accreditation?

- ☐ Yes
- ☐ No

45. Have you developed an accreditation schedule[5]?

- ☐ Yes
- ☐ No

46. How many months do you anticipate TDIF accreditation will take?

47. When do you wish to commence TDIF accreditation?

48. Have you submitted your TDIF accreditation application letter to the Department of Finance?

- ☐ Yes
- ☐ No

49. Has your TDIF accreditation application letter been formally accepted by the Finance?

- ☐ Yes
- ☐ No

Thank you for filling out the TDIF Statement of Claims. If you have any further comments, please enter them in the box below.

[5] The *TDIF Application for Accreditation Letter template* available on the Digital Identity website includes a section for the accreditation schedule.