Digital Identity Accreditation Application Form

Starting your application

This is an application to be accredited as one or more of the following kinds of accredited entities:

- an accredited attribute service provider
- an accredited identity exchange provider
- an accredited identity service provider
- an entity that provides, or proposes to provide, a service of a kind prescribed by the Accreditation Rules.

In making an application for accreditation, the organisation will need to have conducted:

- each kind of assurance assessment
- each kind of systems testing applicable to the accredited services the organisation will provide if accredited; and
- any other testing as required under the Digital ID Accreditation Rules.

We recommend you read the *Digital ID Act 2024*, Digital ID (Accreditation) Rules and our Digital ID Accreditation guidance before commencing your application to ensure you understand your obligations as an accredited entity and the evidence that will be required to complete your application and what each document should contain.

This information is required to assess whether the organisation satisfies the accreditation criteria.

WARNING: It is a serious criminal offence under the Commonwealth Criminal Code to provide false or misleading information. False or misleading information in an application (including a material omission) may also be grounds to revoke any accreditation granted based on that information.

Personal information collection notice

Some of the information you provide in your application for accreditation may constitute personal information for the purposes of the *Privacy Act 1988* and the *Digital ID Act 2024*. This notice is intended to inform you of matters related to our collection of personal information contained in your application and should be read in conjunction with the ACCC's Privacy Policy.

Why we are collecting personal information

Information, including any personal information, contained in your application is being collected by the ACCC as the Digital ID Regulator for the purposes of:

- assessing your application for accreditation in accordance with the *Digital ID Act 2024;* and
- administering, and otherwise facilitating the proper functioning of the *Digital ID Act 2024*.

What happens if you do not provide requested personal information.

If you do not provide personal information relevant to your application for accreditation, that may impact our ability to assess your application.

Whom we may disclose personal information to

Information contained within accreditation applications, including personal information, may be disclosed to:

- other Commonwealth agencies (for example, the Office of the Australian Information Commissioner and the Australian Security Intelligence Organisation);
- State and Territory police forces;
- international regulators and law enforcement bodies;
- external consultants engaged by us

to assist our assessment of accreditation applications.

The information, including any personal information, contained in accreditation applications is collected, and stored on servers, in Australia, in a secure environment. As above, personal information contained in accreditation applications may be disclosed overseas to relevant international regulators and law enforcement bodies to assist our assessment of accreditation applications.

Information about how to access your personal information, how to correct your personal information and how to complain about our handling of your personal information (and how we'll deal with such a complaint) is set out in the ACCC's Privacy Policy.

By ticking the box below, you confirm that you have obtained the consent of any individual to whom personal information contained in your accreditation application relates to disclose their personal information to the ACCC (as the Digital ID Regulator) to be collected, used, and disclosed for the purposes as set out above.

☐ **Yes**

General

*All items marked with an asterisk * are mandatory.*

Documents to upload

Please upload the following documents.

- Statement of scope and applicability *
- Description of the DI Data Environment *
- Evidence of technical testing (including the Requirements Traceability Matrix)
- Technical Testing Attestation statement *

  Please refer to the Digital ID Regulator's guidance for the template forms and more information
- Diagram showing corporate ownership (including percentages) *

Questions

1. Name of the organisation applying for accreditation *

2. Number of employees

   ○ 0-4 ○ 5-19 ○ 20-50 ○ 51-100 ○ 101-199 ○ 200+

3. Please describe the ownership structure of the organisation. Include ownership or shareholder names (companies and individuals), a breakdown of capital and voting rights and detail any close links to other companies (including upstream ownership).

4. Number of owners/shareholders

   ○ 0-4 ○ 5-19 ○ 20+

5. For each direct ownership holding, or indirect holding (fund or trust) greater than 5% of the organisation please populate the following information (where applicable). If you have additional shareholders that do not fit in the below table, please provide details of them separately: *

Name of owners	Ownership %	The level of control, including the types of rights that the owner has, for example, voting rights and veto rights, board rights, access to company information, including personal identifiable information holdings	Date of birth	Country or countries of Citizenship	Country of birth	Country or countries of Residence

6. How is data collected by the organisation stored? *

○ On-premises ○ Data centre ○ In the cloud ○ Other

7. What country or countries, if more than one, is the data stored in? *

8. In which country or countries is the organisation registered, and in which country or countries does the organisation operate? *

Conditions

Your organisation's accreditation is subject to conditions, including the default conditions imposed by the *Digital ID Act 2024*, the Digital ID Rules 2024, and the Digital ID (Accreditation) Rules 2024. This section is intended to cover conditions in addition to those imposed by default, and those imposed by the Digital ID Regulator to define the boundaries of your accreditation.

*All items marked with an asterisk * are mandatory.*

Document upload:

- Supporting evidence for any conditions

Questions

1. Does the condition you want to impose relate to your organisation as a whole or a service your organisation provides? *

   ○ Organisation ○ Service

2. What type of condition do you want to impose? Select the condition sought to be imposed. *

   ○ Conditions relating to any limitations, exclusions or restrictions in relation to the accredited services

   ○ Conditions relating to identity proofing levels

   ○ Conditions relating to authentication levels

   ○ Conditions relating to alterative proofing processes

   ○ Conditions relating to reusable digital IDs

   ○ Conditions relating to one-off digital IDs

   ○ Conditions relating to the circumstances or manner in which the accredited services must be provided

   ○ Conditions relating to special attributes

   ○ Conditions relating to restricted attributes of individuals

   ○ Conditions relating to biometric information of individuals

   ○ Conditions relating to the organisation's information technology systems through which the accredited services are provided

   ○ Conditions relating to the actions the organisation must take before suspending or revoking accreditation

- Other condition

3. If **restricted attributes** is selected as a condition at question 2:

   a. Select the kind or kinds of restricted attributes sought to be collected, disclosed, or collected and disclosed. *

   - Health information (within the meaning of the *Privacy Act 1988*) about an individual
   - An identifier of an individual that has been issued or assigned by or on behalf of the Commonwealth, a State or Territory, an authority or agency of the Commonwealth, a State or Territory, or a government of a foreign country
   - Information or an opinion about an individual's criminal record
   - Information or an opinion about an individual's membership of a professional or trade association
   - Information or an opinion about an individual's membership of a trade union
   - Other information or opinion that is associated with an individual and is prescribed by the Accreditation Rules

   b. Specify which restricted attribute(s) is sought to be collected, disclosed, or collected and disclosed *

   c. Is your organisation seeking to collect, disclose, or collect and disclose a restricted attribute of an individual. *

   Collect   Disclose   Collect and Disclose

   d. If the selection made in step 3c is 'Disclose' or ‘Collect and disclose’, please list the relying party or relying parties your organisation is seeking to disclose a restricted attribute to. *

e. If the selection made in step 3c is 'Disclose' or ‘Collect and disclose’, please outline the arrangements in place between your organisation and each relying party (not including participating relying parties) to ensure the protection of the restricted attribute(s) from further disclosure. *

f. Provide justification as to why the restricted attribute(s) is sought to be collected, disclosed, or collected and disclosed. *

g. Provide an explanation as to why a similar outcome cannot be achieved without the restricted attribute(s) being collected, disclosed, or collected and disclosed. *

h. Specify whether the collection, disclosure, or collection and disclosure of the restricted attribute(s) is regulated by other legislative or regulatory requirements. *

O Yes O No

i. If the answer to the question ‘3h’ is 'Yes', please specify the relevant legislative or regulatory requirement(s). *

j. If the answer to the question '3h' is 'Yes', please provide an explanation as to how your organisation would comply with the legislative or regulatory requirement(s) if the condition were imposed. *

k. When considering whether to impose a condition relating to restricted attributes, the Digital ID Regulator must consider the potential harm that could result if the restricted attributes were disclosed to an organisation that was not authorised to collect them and the community expectations as to whether the restricted attributes must be handled more securely than other kinds of attributes. You may provide any information that you consider relevant to the Digital ID Regulator's consideration of these matters.

4. If the applicant is seeking a condition (not relating to restricted attributes of individuals)

   a. Describe the condition sought to be imposed.

   b. Provide justification as to why the condition is sought to be imposed.

c. Select the desired date of effect for the condition to be imposed, if any.

d. Select the desired date when the condition will cease to be imposed, if any.

If you need to apply for another condition/s please provide the information for each in a Conditions on Accreditation or Approval Form available here.

Evidence it is appropriate to accredit the organisation

Please upload the relevant forms and associated evidence to help us assess whether, in light of the objectives of the *Digital ID Act*, it is appropriate to accredit the organisation.

Please refer to the Digital ID Regulator's guidance for the template forms and more information.

Accreditation criteria

*All items marked with an asterisk * are mandatory.*

Privacy

Please provide the following documents:

- Privacy impact assessment *
- Organisation's response to privacy impact assessment *
- Privacy management plan(s)
- Privacy policy(s)
- Data breach response plan(s)
- Any other document supporting your ability to comply with privacy related requirements.

Questions

1. What is the date of the Privacy Impact Assessment?

2. Name of assessor who completed the Privacy Impact Assessment?

3. Please outline the assessor's experience, training, and qualifications to conduct a Privacy Impact Assessment. *

4. Is the assessor external to the organisation and, if the organisation is part of a corporate group, external to the group? *

   ○ Yes ○ No

   Selecting 'no' means this assessor is ineligible.

5. Has the assessor been involved in the design, implementation, operation or management of the organisation's DI data environment or accredited services? *

   ○ Yes ○ No

   Selecting 'yes' means this assessor is ineligible.

6. What established risk management framework has the organisation used in its response to the Privacy Impact Assessment? *

7. Please indicate where the assessment recommended actions to improve the organisation's ability to comply with the privacy requirements: *

   Tick Applicable boxes

   ☐ compliance with the Privacy (Australian Government Agencies — Governance) APP Code 2017

   ☐ processes for an individual to provide express consent, or to withdraw or vary that consent (for an accredited entity with public-facing accredited services)

   ☐ compliance with the data minimisation principle

   ☐ privacy awareness training for personnel whose duties relate to accredited services or DI data environment

   ☐ processes or actions to be taken by the organisation in the event of a data breach or suspected data breach involving its accredited services or DI data environment

   ☐ other

8. Did the organisation accept and implement all recommendations contained in the Privacy Impact Assessment?

O Yes O No

If no, please ensure your organisation's response to the Privacy Impact Assessment includes an explanation of your reasons.

9. Are there any actions outstanding that were identified in the Privacy Impact Assessment to mitigate any privacy risks? *

O Yes O No

If yes, please ensure your response includes why the actions have not been completed before applying and the timeframe in which the organisation will complete the action.

10. Indicate where your Privacy Policy will be kept to ensure individual consumers can access it.

11. Is there any other information that the organisation would like to provide in relation to privacy?

12. If you uploaded any additional documents, please advise how the document addresses the legislative requirements or otherwise supports your application.

Fraud

*All items marked with an asterisk * are mandatory.*

Please provide the following documents:

- Fraud assessment *
- Organisation's response to fraud assessment *
- Fraud risk assessment *
- Fraud control plan
- Any other document supporting your ability to comply with fraud related requirements

Questions

1. Date of the Fraud Assessment

2. Name of assessor who completed the Fraud Assessment:

3. Please outline the assessor's experience, training and qualifications to conduct the Fraud Assessment. *

4. Is the assessor external to the organisation and, if the organisation is part of a corporate group, external to the group? *

   ○ Yes ○ No

   Selecting 'no' means this assessor is ineligible.

5. Has the assessor been involved in the design, implementation, operation or management of the organisation's DI data environment or accredited services? *

   ○ Yes ○ No

   Selecting 'yes' means this assessor is ineligible.

6. Please indicate where the assessment recommended actions to improve the organisation's fraud control measures:

   Tick applicable boxes

   ☐ [For applicant's seeking to be accredited as an accredited identity service provider] providing advice to individuals regarding how to safeguard their digital ID against current and emerging fraud risks

   ☐ providing support services to individuals who have been adversely affected by a digital ID fraud incident i.e. a monitored chat or email function, and a function that allows the individual to request to speak to a real person

   ☐ the strategies and controls to manage risks, threats and vulnerabilities, including fraud risks eventuating through other entities interacting with the organisation's DI data environment

   ☐ the mechanisms to prevent, detect and alert the organisation's personnel to digital ID fraud incidents

   ☐ the mechanisms for responding to digital ID fraud incidents, including procedures to document organisation's processes for responding to digital ID fraud incidents and how it will investigate such incidents

   ☐ processes to share information on known fraud risks or digital ID fraud incidents with other participants

   ☐ [For applicant's seeking to authority to collect, use and disclose biometric information] mitigation strategies and treatments related to biometric information, including conducting biometric binding or using biometric information for authentication

   ☐ [For applicant's seeking to authority to collect, use and disclose biometric information] for organisations using biometric information of an individual for the purposes of preventing or investigating a digital ID fraud incident, ethical principles aimed at avoiding disadvantage to, or discrimination against, individuals

   ☐ fraud awareness training for personnel whose duties relate to the organisation's accredited services or DI data environment

7. Did the organisation accept and implement all recommendations contained in the Fraud Assessment?

   ○ Yes ○ No

   If no, please ensure your response to the Fraud Assessment includes an explanation of your reasons.

8. Are there any actions outstanding that were identified in the Fraud Assessment. *

   O Yes   O No

   If yes, please ensure your response includes why the actions have not been completed before applying and the timeframe in which the organisation will complete the action.

9. Is there any other information that the organisation would like to provide in relation to fraud controls?

10. If you uploaded an additional document, please advise how the document addresses the legislative requirements or otherwise supports your application.

Protective security

*All items marked with an asterisk * are mandatory.*

Please provide the following documents:

- Protective Security Assessment *
- Organisation's response to Protective Security Assessment *
- Cyber security risk assessment *
- System security plan
- Cloud services management plan
- Cloud services providers register
- Penetration testing report *
- Essential strategies review report
- Disaster recovery and business continuity plan
- Logging implementation and monitoring plan
- Any other document supporting your ability to comply with protective security requirements.

Questions

1. Protective Security Assessment
   a. Date the Protective Security Assessment was completed

   b. Which standard or framework has the organisation chosen to comply with: ISO 27001, PSPF or an alternative? *

   ○ ISO 27001 ○ PSPF ○ Alternative

   c. Please outline the experience, training and qualifications of the assessor: *

   d. Is the assessor external to the organisation and, if the organisation is part of a corporate group, external to the group? *

   ○ Yes ○ No

   Selecting 'no' means this assessor is ineligible.

e. Has the assessor been involved in the design, implementation, operation or management of the organisation’s DI data environment or accredited services? *

○ Yes ○ No

Selecting ‘yes’ means this assessor is ineligible.

f. If the organisation considers a particular protective security control or essential eight strategy is not relevant to the organisation, has the assessor included their responding opinion in the Protective Security Assessment?

○ Yes ○ No

g. Please indicate where the assessment recommended actions to improve the organisation’s protective security controls:

Tick applicable boxes

☐ maintenance and compliance with requirements of a Disaster Recovery and Business Continuity Plan

☐ maintenance and compliance with requirements of a System Security Plan

☐ maintenance and compliance with requirements of Logging implementation and monitoring plan

☐ [For applicant’s intending to use cloud services as part of its DI data environment] maintenance and compliance with requirements of Cloud Services Management Plan

☐ [For applicant’s intending to use cloud services as part of its DI data environment] requirements of the Cloud Service Providers Register in the Digital ID (Accreditation) Rules

☐ processes to ensure that all digital ID information collected, used, held or disclosed by or on behalf of the accredited entity is protected in transit, and at rest, by approved cryptography, including compliance with cryptographic standards in the Australian Government Information Security Manual

☐ Cryptographic key management processes and procedures

☐ [For applicant’s seeking to authority to collect, use and disclose biometric information] use of Biometric information for testing

☐ [For applicant’s intending to provide identity proofing] identity proofing processes

☐ [For applicant’s intending to provide authentication services] authentication services

☐ approach to ensuring the ongoing eligibility and suitability of the organisation’s personnel who interact with its DI data environment

☐ implementation and compliance with the ‘Essential Eight Maturity Model to ISM Mapping’ document for ISM controls marked Maturity Level two.

h. Did the organisation accept and implement all recommendations contained in the Protective Security Assessment?

O Yes O No

If no, please ensure your response to the Protective Security Assessment includes an explanation of your reasons.

i. Are there any actions outstanding that were identified in the protective security assessment to address protective security requirements in the Digital ID (Accreditation) Rules? *

O Yes O No

If yes, please ensure your response includes why the actions have not been completed before applying and the timeframe in which the organisation will complete the action.

j. Is there any further information that you would like to provide in relation to Protective Security requirements?

k. If you uploaded an additional document, please advise how the document addresses the legislative requirements or otherwise supports your application.

2. Cyber security risk assessment:

a. Date of the Cyber Security Risk Assessment

b. What established risk management framework has the organisation used to develop its cyber security risk matrix? *

c. Please indicate where the assessment recommended actions to improve the organisation's response to cyber security risks and incidents:

Tick applicable boxes

☐ sharing information on the known cyber security risks with the other participants in the Digital ID scheme

☐ notifying other relevant entities involved in the digital ID system of an incident, risk or breach

☐ [For applicant's seeking to be accredited as an accredited identity service provider] providing advice to individuals regarding how to safeguard their digital ID against current and emerging cyber security risks

☐ providing support services to individuals who have been adversely affected by a cyber security incident

☐ mechanisms to prevent and detect cyber security incidents

☐ mechanisms for investigating or otherwise dealing with cyber security incidents

☐ processes to identify and suspend or prevent use of the digital IDs or attributes (including special attributes) affected by cyber security incidents

☐ cyber security incident record keeping processes

☐ compliance with the mitigation strategies whose 'relative security effectiveness rating' is marked 'essential' in the Strategies to Mitigate Cyber Security Incidents document published by the Australian Cyber Security Centre

d. Are there any actions outstanding that were identified in the cyber security risk assessment to address cyber security risks associated with the organisation's accredited services and DI data environment? *

Yes No

If yes, please ensure your response includes why the actions have not been completed before applying and the timeframe in which the organisation will complete the action.

3. Penetration testing:

a. Date of the penetration testing

Note: the penetration testing must be conducted before the protective security assessment.

b. Name of assessor who completed the penetration testing.

c. Please outline the experience, training and qualifications of the assessor: *

d. Is the assessor external to the organisation and, if the organisation is part of a corporate group, external to the group? *

Yes No

Selecting 'no' means this assessor is ineligible.

e. Has the assessor been involved in the design, implementation, operation or management of the organisation's DI data environment or accredited services? *

Yes No

Selecting 'yes' means this assessor is ineligible.

f. Did the organisation review and address all the results of the penetration testing report?

O Yes O No

If no, please explain your reasons.

g. Are there any actions outstanding that were needed to address the results of the Penetration test report?

O Yes O No

If yes, please explain why the actions have not been completed before applying and the timeframe in which the organisation will complete the action.

Accessibility and useability

*All items marked with an asterisk * are mandatory.*

Provide the following documents:

- Accessibility and useability assessment *
- Organisation's response to accessibility and useability assessment *
- Useability testing report
- WCAG testing report
- Any other document supporting your ability to comply with accessibility and useability related requirements.

Questions

1. Date the accessibility and useability assessment was completed.

2. Name of assessor who completed the accessibility and useability assessment.

3. Outline the experience, training and qualifications of the assessor regarding their ability to conduct the assessment. *

4. Please indicate where the assessment recommended actions to improve accessibility and useability:

   Tick all applicable

   ☐ providing individuals with information related to the organisation's accredited services

   ☐ providing assisted digital support to individuals who may experience barriers when creating or using a digital ID (for entities with public-facing services)

   ☐ processes and procedures to enable individuals to seek assistance or otherwise resolve disputes or complaints (for entities with public-facing services)

   ☐ processes and procedures for obtaining, recording and actioning feedback from individuals about the accessibility and useability of the accredited service to be provided by the organisation (for entities with public-facing services)

☐ design and useability of the organisation's public-facing DI data environment for users or expected users of the organisation's accredited services

☐ [For applicant's seeking to be accredited as an accredited identity service provider] the organisation's implementation and compliance with the user experience requirements regarding identity proofing processes

☐ [For applicant's seeking to be accredited as an accredited identity service provider] providing information to users about the use and maintenance of authenticators

☐ [For applicant's seeking to be accredited as an accredited identity service provider] the organisation's implementation and compliance with the user experience requirements regarding reusable digital IDs

☐ the scope or findings of WCAG testing

☐ the scope or findings of useability testing

5. Did the organisation accept and implement all recommendations contained in the accessibility and useability assessment?

O Yes O No

If no, please ensure your response to the accessibility and useability assessment includes an explanation of your reasons.

6. Are there any actions outstanding that were identified in the accessibility and useability assessment? *

O Yes O No

If yes, please ensure your response includes why the actions have not been completed before applying and the timeframe in which the organisation will complete the action.

7. Please explain any actions and changes implemented as a result of the WCAG testing report.

8. Please explain any actions and changes implemented as a result of the Useability testing report

9. Is there any other information that the organisation would like to provide in relation to accessibility and useability requirements?

10. If you uploaded an additional document, please advise how the document addresses the legislative requirements or otherwise supports your application.

Role Specific Accreditation criteria

Biometrics

This section of the application form is applicable to applicant's seeking authority to collect, use and disclose biometric information.

For applicants completing this section, the asterisk * indicates a mandatory field.

Please provide the following documents:

- Biometric binding processes
- Test plan and processes (as required)
- Ethical policies and procedures (as required)
- Presentation attack detection technology report *
- Biometric matching algorithm testing report
- Evidence of source biometric matching testing
- eIDVT testing report
- Any other document supporting your ability to comply with biometric related requirements.

Questions

1. What method(s) does the organisation intend to use for online biometric binding:

   Tick applicable boxes

   ☐ technical biometric matching

   ☐ source biometric matching

   ☐ eIDVT biometric matching

2. What method(s) does the organisation intend to use for local biometric binding performed by an assessing officer in the physical presence of the individual:

   Tick applicable boxes

   ☐ technical biometric matching

   ☐ source biometric matching

   ☐ eIDVT biometric matching

   ☐ manual face comparison

3. Biometric matching algorithm test report for technical biometric matching

    a. What is the date of the biometric matching algorithm test report?

    b. Name of the laboratory which completed the biometric matching algorithm test report?

    c. Please outline the laboratory personnel's relevant experience, training and qualifications to conduct a biometric matching algorithm test report

    d. Is the assessor external to the organisation and, if the organisation is part of a corporate group, external to the group?

    O Yes O No

    Selecting 'no' means this biometric matching algorithm report is ineligible.

    e. Has the assessor been involved in the design, implementation, operation or management of the organisation's DI data environment or accredited services?

    O Yes O No

    Selecting 'yes' means this biometric matching algorithm report is ineligible.

    f. Does the biometric matching algorithm test report confirm the results are within the Digital ID (Accreditation) Data Standards 2024 thresholds?

    O Yes O No

4. [For applicant's intending to use eIDVT matching] eIDVT testing report:

    a. What is the date of the eIDVT testing report?

b. Name of laboratory which completed the eIDVT testing report?

c. Please outline the laboratory personnel's relevant experience, training and qualifications eIDVT testing.

d. Does the eIDVT test report confirm that eIDVT was tested according to the requirements of the Accreditation Data Standards?

O Yes O No

If yes, does the eIDVT test report confirm that the testing met the requirements of the Accreditation Data Standards?

O Yes O No

If no, please provide details of non-conformances and the organisation's response to the eIDVT test findings

5. Presentation attack detection technology report:

a. What is the date of the Presentation attack detection technology report?

b. Name of laboratory which completed the Presentation attack detection technology report

c. Please outline the assessor/laboratory personnel's relevant experience, training and qualifications to conduct Presentation attack detection testing.

d. Is the assessor external to the organisation and, if the organisation is part of a corporate group, external to the group?

O Yes O No

Selecting 'no' means this is an ineligible assessor.

e. Has the assessor been involved in the design, implementation, operation or management of the organisation's DI data environment or accredited services?

O Yes O No

Selecting 'yes' means this is an ineligible assessor.

f. Does the test report confirm that the organisation's presentation attack detection technology has been tested in accordance with the relevant requirements of ISO 30107-3?

O Yes O No

g. Are there any actions outstanding that were identified in the Presentation attack detection technology report?

O Yes O No

6. Authentication services using biometric information

a. Does the organisation intend to use biometric information to provide Authenticator services?

O Yes O No

Note: *If the answer to 6a is "No", then questions 6b, 6c, and 6d are not required.*

b. What does the organisation intend to use for authentication?

- in-device biometric capability

  O Yes O No

- custom biometric capability

  O Yes O No

c. Are there any actions outstanding that address any risks, threats and vulnerabilities specific to the use of in-device capability identified in the organisation's fraud control plan?

O Yes O No

d. If yes, please explain why the actions have not been completed before applying and the timeframe in which the organisation will complete the action.

e. Was the organisation's biometric matching algorithm regarding the use of custom biometric capabilities tested by a biometric testing entity?

O Yes O No

Identity proofing

This section of the application form is applicable for applicants seeking to provide identity proofing services.

Provide the following documents:

- Identify proofing process
- Event logging implementation & monitoring plan
- Any other document supporting your ability to comply with identify proofing requirements.
- [For applicant's seeking to provide alternative proofing] Risk assessment for use of alternative proofing process

Questions

1. For the highest level of identity proofing being applied for, does the organisation: *Tick applicable boxes*

   ☐ require the individual applying for a digital ID to have a unique username

   ☐ establish that the identity is unique

   ☐ establish that the identity is not that of a deceased person

   ☐ verify the link between the identity through biometric binding

   ☐ require the individual to provide original, physical documents or other credentials in person

   ☐ ensure the identity is not known to be used fraudulently

   ☐ provide tools and training to personnel undertaking identity proofing processes, to detect fraudulent attributes, and documents or other credentials before starting work on these duties and annually thereafter

   ☐ provide National Accreditation Authority for Translators and Interpreters (NAATI) accredited translation of documents or other credentials

   ☐ require attributes to be verified using source or technical verification

   ☐ undertake verification of a COI credential

   ☐ undertake verification of a photo ID

   undertake verification of a UiTC credential if attributes vary across documents or other credentials

   ☐ Once

   ☐ Twice

   ☐ Never

   ☐ undertake verification of a linking credential.

2. For an organisation intending to use an alternative proofing process

   a. Which proofing level is the alternative proofing level equivalent to.

      ○ IP1 ○ IP Plus ○ IP2 ○ IP2 Plus ○ IP3

      ○ IP4

   b. Please indicate if the organisation's alternative proofing process include any of the following:

      Tick applicable boxes

      ☐ acceptance of alternative types of credentials

      ☐ verification of an individual's claimed identity with an individual who is a trusted referee and whose identity has been verified to an equal or greater identity proofing level than the level requested

      ☐ verification of an individual's claimed identity with a reputable organisation known to the individual

      ☐ reliance on the identity proofing processes of other organisations that have verified the identity of the individual to the relevant identity proofing level

      ☐ an interview with the individual to assess the consistency and legitimacy of the individual's claims, and the validity of the claimed identity

      ☐ alternative methods for individuals to provide attributes or credentials to the organisation

      ☐ providing support for individuals to obtain evidence which, without limitation, may include assisting an individual to register their birth.

      ☐ another process

Authentication management

This section of the application form is applicable for applicants seeking to Authentication management services.

Provide the following documents:

- Cryptographic key management processes and procedures
- Any other document supporting your ability to comply with authentication requirements

Questions

1. Use the tick box to select each kind of authenticator the organisation will be utilising when providing authentication services:

   Tick applicable boxes

   ☐ memorised secret

   ☐ single factor cryptographic device

   ☐ look-up secret

   ☐ multi factor one time password device

   ☐ out-of-band device

   ☐ multi factor cryptographic software

   ☐ single factor one time password device

   ☐ multi factor cryptographic device

   ☐ single factor cryptographic software

   ☐ other

2. Describe how an individual can access information about the use and maintenance of their authenticators and provide a link to where information is located.

3. If the organisation will be utilising physical authenticators, Describe the process to revoke or suspend the authenticator if it is suspected to be lost or stolen.

Accredited identity service providers

This section of the application form is applicable for applicants seeking to be accredited as an accredited identity service provider.

Provide the following documents:

- System design
- Any other document supporting your ability to comply the identify service provider requirements

Questions

1. Does the organisation have a process in place to ensure that it does not generate, manage, maintain or verify information of an individual if the individual has not yet attained the age of 15 years?

   Yes No

2. [if relevant] Will the Identity Service Provider generate and verify one-off digital IDs?

   Yes No

   If yes, how will the Identity Service Provider ensure that it does not retain an attribute of an individual once the attribute has been disclosed to the relying party in a transaction, unless the ISP is required to retain this attribute by law?

Accredited identity exchange providers

This section of the application form is applicable for applicants intending to operate a digital ID system, other than the Australian Government Digital ID System and where one of more digital ID service providers makes available services that are not accredited services.

For applicants completing this section, the asterisk * indicates a mandatory field'.

Provide the following documents:

- Digital ID system Rules (for private organisations only)
- System design *
- Any other document supporting your ability to comply with identity exchange provider requirements

Questions

1. Please indicate whether the Digital ID System Rules:

   ☐ are binding on an identity service provider that provides services in the digital ID system that are not accredited services (unaccredited identity service provider)

   ☐ are enforceable to the extent that the identity exchange provider, or another person is able to enforce the Digital ID system rules and can revoke the unaccredited identity service provider's participation in the Digital ID system for non-compliance with the Digital ID system rules

   ☐ are consistent with the *Digital ID Act* and the Digital ID (Accreditation) Rules

   ☐ require that all information conveyed or managed within the system is dealt with in accordance with approved cryptography as per the Digital ID (Accreditation) Rules as they apply to the unaccredited identity service provider

   ☐ require that an unaccredited identity service provider participating in the Digital ID system must not disclose an attribute of an individual without the express consent of the individual, unless permitted by the *Digital ID Act*.

   ☐ prohibit one-to-many matching of biometric information of an individual

Finalise application

Review

Please review the information that you have provided and amend if required.

WARNING: It is a serious criminal offence under the Commonwealth Criminal Code to provide false or misleading information. False or misleading information in an application (including a material omission) may also be grounds to revoke any accreditation granted based on that information.

Additional information

1. Is there anything additional that you want to provide us before you submit your application?

   For example, information that may assist with the assessment of your application, or further information of interest.

Confirm your address

2. Are the organisation's address details for the giving of notices and other documents under the Digital ID framework, up to date?

   ○ Yes ○ No (Go to question 3)

3. Complete the following to update the organisation's address details for the giving of notices and other documents under the Digital ID framework:

   Organisation's email address

   Note: the organisation must notify the Digital ID Regulator if the organisation has withdrawn any consent to notices and other documents under the Digital ID framework being given by email.

Organisation’s physical address

Organisation’s postal address

The organisation must notify the Regulator in writing of any change to the organisation’s address details as soon as practicable after the change occurs.

Declaration

If you need someone else to complete this, please refer to the Digital ID Regulator's guidance for the template forms and upload.

- I declare that I have been authorised by my organisation to make the declarations and attestations contained in this application.
- I declare that all the information that I have provided in this application, including any documents, is complete and correct.
- I understand that, if accredited, my organisation will be required to comply with all the requirements in the *Digital ID Act*, Digital ID Rules, Accreditation Rules and Accreditation Data Standards. This includes an obligation to notify the Digital ID Regulator of ‘reportable incidents’, and to submit annual reports for each reporting period.
- I declare that my organisation is not aware of any circumstances that might prevent or adversely affect its ability to comply with the *Digital ID Act*, the Digital ID Rules, Accreditation Rules or the Accreditation Data Standards.

Signed:	Date: