02 - Overview

Trusted Digital Identity Framework Release 4
February 2021, version 1.2

PUBLISHED VERSION
Digital Transformation Agency (DTA)

This work is copyright. Apart from any use as permitted under the Copyright Act 1968 and the rights explicitly granted below, all rights are reserved.

Licence

With the exception of the Commonwealth Coat of Arms and where otherwise noted, this product is provided under a Creative Commons Attribution 4.0 International Licence. (http://creativecommons.org/licenses/by/4.0/legalcode)

This licence lets you distribute, remix, tweak and build upon this work, even commercially, as long as they credit the DTA for the original creation. Except where otherwise noted, any reference to, reuse or distribution of part or all of this work must include the following attribution:

Trusted Digital Identity Framework (TDIF)™: 02 - Overview © Commonwealth of Australia (Digital Transformation Agency) 2020

Use of the Coat of Arms

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

Conventions

References to TDIF documents, abbreviations and key terms (including the words MUST, MUST NOT, and MAY) are denoted in italics are to be interpreted as described in the current published version of the TDIF: 01 – Glossary of Abbreviations and Terms.

TDIF requirements and references to Applicants are to be read as also meaning Accredited Participants, and vice versa. The scope of TDIF requirements are to be read as applying to the identity system under Accreditation and not to the organisation’s broader operating environment.

Contact us

The DTA is committed to providing web accessible content wherever possible. This document has undergone an accessibility check however, if you are having difficulties with accessing the document, or have questions or comments regarding the document please email the Director, Digital Identity Policy at identity@dta.gov.au.
Document management

The DTA has endorsed this document for release.

Change log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Description of the changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>July 2019</td>
<td>SJP</td>
<td>Initial version</td>
</tr>
<tr>
<td>0.2</td>
<td>Oct 2019</td>
<td>SJP</td>
<td>Updated to incorporate feedback provided by stakeholders during the first round of collaboration on TDIF Release 4</td>
</tr>
<tr>
<td>0.3</td>
<td>Dec 2019</td>
<td>SJP</td>
<td>Updated to incorporate feedback provided by stakeholders during the second round of collaboration on TDIF Release 4</td>
</tr>
<tr>
<td>0.4</td>
<td>Mar 2020</td>
<td>SJP</td>
<td>Updated to incorporate feedback provided during the public consultation round on TDIF Release 4</td>
</tr>
<tr>
<td>1.0</td>
<td>May 2020</td>
<td></td>
<td>Published version</td>
</tr>
<tr>
<td>1.1</td>
<td>Jul 2020</td>
<td>SJP</td>
<td>Updated references</td>
</tr>
<tr>
<td>1.2</td>
<td>Feb 2021</td>
<td>JK</td>
<td>CRID0001 – Updated references, added requirements subject area description table. CRID0003 – minor grammar and style update.</td>
</tr>
</tbody>
</table>

Document review

The next scheduled review of this document will occur by July 2022. Any changes made to the document prior to this date will be recorded in a TDIF change management document and published to the DTA website.
Introduction

The DTA has been developing the TDIF since 2015. The TDIF is an Accreditation regime which specifies the minimum requirements that Attribute Service Providers, Credential Service Providers, Identity Exchanges and Identity Service Providers are required to meet in order to achieve and maintain TDIF accreditation. This document provides an overview of the TDIF including its scope and objectives.

The intended audience for this document includes:

- Accredited Participants.
- Applicants.
- Assessors.
- Relying Parties.
Trusted Digital Identity Framework

2.1 Early history

The Australian Government has been exploring the concept of online trust for several years.

In 2010 the Australian Government Department of the Prime Minister and Cabinet (PMC) identified a need to strengthen identity management in the digital economy and a voluntary trusted identity model was seen as a possible way to achieve this. The possible model involved the development of a market in identity authentication products which led to the development of the National Trusted Identities Framework (NTIF) in 2011. The aim of the framework was to make it simpler for government and business to confirm the identity of individuals they do business with and allow individuals to verify the credentials of the businesses they transact with online using the same system. PMC conducted two consultation sessions during 2011 and 2012 on the NTIF. Although the sessions identified several issues and questions related to online trust and what might be needed to address it, there was no clear consensus on what next steps should be taken to progress the NTIF.

In 2011 the then Department of Broadband, Communications and the Digital Economy published the National Digital Economy Strategy (NDES), which outlined the government’s vision for Australia’s digital economy. The NDES aimed to improve online government service delivery and engagement and built on the concepts established in the NTIF around online trust.

In 2013 these concepts were explored further, when the Australian Government Information Management Office (AGIMO) published the Third Party Identity Services Assurance Framework (TPISAF). This framework set out the compliance criteria and accreditation requirements for third party providers of identity services. The underlying premise of the framework is that, based on an understanding of an agency requirements, individuals will be able to choose to use the services of an accredited service provider in order to access online government services.
2.2 Recent history

The Australian Government established the Financial System Inquiry\(^1\) (FSI) in December 2013 to examine the positioning of the financial system to meet evolving needs and support economic growth for Australia. In December 2014, the FSI concluded that:

“The innovative potential of Australia’s financial system and broader economy can be supported by taking action to ensure policy settings facilitate future innovation that benefits consumers, business and government”.

To facilitate innovation, the FSI’s recommendations include the aim to:

“Strengthen Australia’s digital identity framework through the development of a national strategy for a federated-style model of trusted digital identities”.

In accepting the recommendations of the FSI in October 2015, the Australian Government agreed that a national digital identity strategy would streamline people’s interactions with government and provide efficiency improvements. As per Inquiry Recommendation 15 (digital identity), the Government also agreed to:

“Work across government and with the private sector to develop a Trusted Digital Identity Framework to support the Government’s Digital Transformation Agenda”.

The TDIF builds on previous trust framework development efforts and responds directly to the FSI and government commitment. The TDIF requires providers of identity-related services to be accredited and establishes the rules for the Australian Government’s identity federation.

2.3 Guiding principles

The TDIF supports the following guiding principles:

\(^1\) See References for further information on the FSI
User centric:

- Accessing digital services must be easy, convenient, simple, secure and trusted.
- *Individuals* can choose to create a *Digital Identity* from a range of accredited government and private sector providers.
- *Individuals* can use one or more *Identity Service Providers* to maintain separate or merged personal and business *Digital Identities*.

Voluntary and transparent:

- *Individuals* choose to participate or not (i.e. opt-in).
- *Individuals* can control their *Digital Identity* in an easy and straightforward manner.
- Records of *Credential use* are maintained securely by *Accredited Participants* and easily accessible by those authorised to do so under the *TDIF*.

Service delivery focused:

- *Accredited Participants* offer choice and convenience for *Users*.
- Participation is cost neutral for *Users*.
- The supporting business model encourages private sector participation.

Privacy enhancing:

- *Personal Information* is only collected and disclosed by *Accredited Participants* with the *Consent of Users* and in accordance with privacy laws and good privacy practices.
- Privacy enhancing technology, policy and processes are applied by *Accredited Participants* to all *Personal Information*.
- *Users* have an informed understanding of how their *Personal Information* will be used and protected.
- *Users* can view and manage their *Personal information*, correct errors and revoke their *Consent*. 
Collaborative:

- Active collaboration between the public and private sectors and the broader community will draw on the respective strengths and expertise of government and business.

Interoperable:

- Facilitate interconnectedness with other Trust Frameworks and identity services nationally and internationally.
- Scalable to grow and accommodate the needs of Accredited Participants and Relying Parties.

Adaptable:

- Promote flexibility and innovation in technology and business models.
- The TDIF is flexible to evolve to meet community expectations and changing business, technology, legal and social needs.
- The TDIF supports secure information exchanges ranging from low to high value and from pseudonymous to fully verified identity proofing.

Secure and resilient:

- Accredited Participants meet stringent government security standards.
- The same Accreditation requirements apply to government agencies and organisations.
- Cyber security threats and risks are identified and actively managed by Accredited Participants and Relying Parties.
- Effective Fraud management controls are implemented and maintained.

2.4 Objectives

Based on the above principles, the TDIF will facilitate the following outcomes:

Simple, easy to use and trusted: A Digital Identity that Individuals want to use.

Accessible: Digital Identity that is accessible to all Individuals regardless of their location, circumstances, abilities or the computing devices they use.
**Secure and privacy-preserving:** Digital Identity is secure and privacy preserving. No single identifier is issued by the Identity Exchange to Identity Service Providers, Attribute Service Providers or Relying Parties. There is no single Credential or centralised database of Personal Information. Individuals are given greater control over their Personal Information and who their Personal Information is shared with. Safeguards and recovery mechanisms are implemented in the event an Individual’s Digital Identity is compromised.

**Standards based:** Digital Identity services support open standards to facilitate interoperability including with other jurisdictions and Trust Frameworks.

### 2.5 Accredited roles

The TDIF supports the Accreditation of Attribute Service Providers, Credential Service Providers, Identity Exchanges and Identity Service Providers.

#### 2.5.1 Attribute Service Providers

Attribute Service Providers generate and manage Attributes and claims that are provided to Relying Parties to support their decision-making processes.

#### 2.5.2 Credential Service Providers

Credential Service Providers generate, bind and distribute Credentials to Individuals or can include the binding and management of Credentials generated by Individuals. This function may also be undertaken by an IdP.
2.5.3 Identity Exchanges

Identity Exchanges conveys, manages and coordinates the flow of identity Attributes and assertions between members of an Identity Federation.

2.5.4 Identity Service Providers

An Identity Service Provider creates, maintains and manages identity Information of Individuals and offers identity-based services.

2.6 Unaccredited roles

Other roles within an Identity Federation (which are not accredited) include Relying Parties, Attribute Verification Services and Users.

2.6.1 Relying Parties

Relying Parties are the organisations that rely on verified Attributes or Assertions provided by Identity Service Providers and Attribute Service Providers to enable the provision of a digital service.

2.6.2 Attribute Verification Services

Attribute Verification Services (also known as an Identity Matching Service) are repositories recognised by the DTA that confirm the veracity of Attributes and associated information. Attribute Verification Services can refer to either the repositories themselves, or the methods used to access them (e.g. Document Verification Service and the Face Verification Service).

2.6.3 Users

Users are Individuals who establish a Digital Identity to obtain digital services from Relying Parties. This includes Individuals acting in their own capacity and Individuals who act on behalf of others.
2.7 Accreditation governance

Currently a series of Memorandums of Understanding (MOU) are in place between the DTA and Accredited Participants. Under these MOUs, the DTA, as part of the Oversight Authority, is responsible for the Accreditation of Applicants and the ongoing accreditation of Participants (Accredited Participants). In time these will be replaced with a set of Operating Rules.

2.8 Accreditation process

TDIF Accreditation is a formal process through which Applicants demonstrate their ability to meet specific requirements to the satisfaction of the DTA. TDIF Accreditation covers the initial accreditation and ongoing accreditation obligations.

**Initial Accreditation:** Accreditation of an Applicant’s identity system is fundamental to its trustworthiness and its functional effectiveness. The TDIF Accreditation Process involves a combination of documentation, third party evaluations by Assessors and operational testing that Applicants must complete to the satisfaction of the DTA to achieve TDIF Accreditation.

**Ongoing Accreditation obligations:** Accredited Participants are required to continue to comply with the requirements of the TDIF to maintain Accreditation. Accredited Participants are required to complete Annual Assessments against the TDIF by the anniversary of their initial Accreditation date and remediate any adverse findings in timeframes agreed with the DTA. These Annual Assessments ensure Accredited Participants continue to meet the requirements of the TDIF.

2.9 TDIF Accreditation Process roles

2.9.1 Applicant and Accredited Participant

The Applicant is responsible for:

- Formally requesting TDIF Accreditation for its identity system from the DTA.
- Preparing all required documentation within timeframes agreed with the DTA.
• Obtaining all relevant internal system *Accreditations* or endorsements from the appropriate *Accountable Authority* throughout the *TDIF Accreditation Process*.
• Completing the required *Functional Assessments* by *Assessors*.
• The provision of all relevant *Accreditation evidence* to the *DTA*.
• Remediating all identified non-conformance and adverse findings to the satisfaction of the *DTA*.
• Accepting the residual risk relating to its identity system. (Residual risks may be accepted by appropriate *Accountable Authority*).
• Responding to all requests for information by the *DTA* in relation to *Accreditation* matters.
• As required by the *DTA*, enter into an agreement with the *DTA* following *TDIF Accreditation*.
• Maintain *Accreditation* in accordance with its agreement.
• Undergo *Annual Assessments* on its identity system by the anniversary of its initial *Accreditation* date as set out in *TDIF: 07 – Annual Assessment*.
• Formally advising the *DTA* of its intention to leave the *TDIF* in the event it:
  o No longer wants to undergo the *TDIF Accreditation Process* or maintain *Accreditation*.
  o Can no longer comply with *TDIF* requirements once accredited.
  o Chooses to no longer maintain its *Accreditation*.

### 2.9.2 Digital Transformation Agency

The *DTA* is responsible for:

• Performing the roles and functions of the *Oversight Authority* in relation to *TDIF Accreditation*.
• Ensuring that the *TDIF Accreditation Process* is conducted with due care and in accordance with the published *TDIF* documents.
• Reviewing, within agreed timeframes, all relevant *Applicant* and *Accredited Participant* evidence to ensure conformance to the published *TDIF* documents.
• Handling and treating all Applicant and Accredited Participant evidence consistent with its classification and sensitivity. Unless otherwise agreed between the Applicant and the DTA, all evidence provided to the DTA will be treated as OFFICIAL information. All DTA Personnel associated with Accreditation activities have an appropriate security clearance level to handle sensitive or classified documents provided to the DTA in relation to TDIF Accreditation.

• Protecting all information provided to it by an Applicant (including their TDIF Accreditation Letter and supporting information), and Accredited Participant to ensure it is only available to staff directly involved with their Accreditation. Any documentation requested by other parties will only be shared with the express permission of the Applicant or Accredited Participant.

• Considering all reports and recommendations from Assessors.

• Interpreting conformance against TDIF requirements.

• All decisions in relation to the initial Accreditation of an Applicant or ongoing accreditation of an Accredited Participant.

• Granting accreditation to an Applicant.

• Maintaining the list of Accredited Participants.

• Maintaining the TDIF Accreditation Register.

• Reviewing all documentation which supports an Accredited Participant’s Annual Assessment.

• Directing Accredited Participants to undergo TDIF Reaccreditation (as required).

• Revoking the accreditation of an Accredited Participant.

2.9.3 Assessors

Assessors are independent evaluators of business processes, documentation, systems and services who have the required skills, experience and qualifications to determine whether an Applicant or Accredited Participant has met specific TDIF requirements.

2 Available on the TDIF website (https://www.dta.gov.au)
As part of the TDIF Accreditation Process, the Applicant is required to undergo a series of Functional Assessments by suitably skilled and experienced Assessors. Assessors are responsible for assessing the Applicant’s compliance against specific TDIF requirements² and documenting their findings.

2.10 Documents

The TDIF documents are grouped into three categories – governance, requirements and guidance.

**Governance documents** – the primary purpose of these documents is to control and direct Accreditation effort.

- TDIF: 01 - Glossary of Abbreviations and Terms, which includes a list of acronyms and a definition of key terms used in the TDIF.
- TDIF: 03 - Accreditation Process, which sets out the process and requirements an Applicant is required to complete to achieve TDIF accreditation.
- TDIF: 06D – Attribute Profile, which describes the Attributes used within the Australian Government’s identity federation and how these are mapped in the OpenID Connect 1.0 Profile and SAML 2.0 Profile.

**Requirements documents** – the purpose of these documents is to set out the TDIF Accreditation requirements to be met by Applicants and Accredited Participants.

- TDIF: 04 - Functional Requirements, which includes requirements applicable to the Accredited Roles, including fraud control, privacy, protective security, user experience and technical testing. This document also includes a series of Functional Assessments to be undertaken by the Applicant to achieve TDIF accreditation, including a Privacy Impact Assessment, Privacy Assessment, Security assessment, penetration test and an assessment against the Web Content Accessibility Guidelines.
- TDIF: 05 - Role Requirements, which includes user terms and lifecycle management requirements applicable to the Accredited Roles.

² See TDIF: 04 - Functional Requirements for further information.
• **TDIF: 06: Federation Onboarding Requirements**, which includes the requirements to be met when an Applicant’s identity system is approved to onboard to the Australian Government’s identity federation. This document includes functional requirements, technical integration testing requirements, operating obligations and the accreditation requirements for an Identity Exchange.¹

• **TDIF: 06B - OpenID Connect 1.0 Profile**, which describes how OpenID Connect 1.0 is used within the Australian Government’s identity federation.

• **TDIF: 06C - SAML 2.0 Profile**, which describes how SAML 2.0 is used within the Australian Government’s identity federation.

• **TDIF: 07 - Annual Assessment**, which sets out the process and requirements an Accredited Participant is required to complete by the anniversary of their initial accreditation date to remain TDIF accredited.

**Guidance documents** – the purpose of these documents is to set out information to help Applicants and Accredited Participants meet TDIF requirements.

• **TDIF: 02 - Overview**, (this document) which provides a high-level overview of the TDIF.

• **TDIF: 04A – Functional Guidance**, which provides guidance to Applicants on meeting the requirements set out in **TDIF: 04 Functional Requirements**.

• **TDIF: 05A – Role Guidance**, which provides guidance to Applicants on meeting requirements set out in **TDIF: 05 Role Requirements**.

• **TDIF: 06A – Federation Onboarding Guidance**, which provides guidance to Applicants on meeting requirements set out in the **TDIF: 06 Federation Onboarding Requirements**.

¹ The Identity Exchange performs a unique role in the identity federation. Where other Accredited Roles are standalone systems, the Identity Exchange needs to demonstrate how it coordinates the flow of data to other Participants. For this reason, the Identity Exchange Accreditation requirements are listed in **TDIF: 06 - Federation-onboarding Requirements** and not the **TDIF: 05 - Role Requirements**.
2.11 Requirements schema

The following is an example of a TDIF requirement:

**TDIF Req:** ACCRED-03-01-01; **Updated:** Mar-20; **Applicability:** A, C, I, X

The Applicant **MUST** formally request TDIF accreditation and complete the **TDIF Application Letter** at Appendix A. Each TDIF requirement includes the following information.

- **TDIF Req:** The unique identifier for each TDIF requirement.
  
  Each TDIF requirement uses the following schema
  
  `[Subject Area -Document Section – Requirement -Sub Requirement].`
  
  - **Subject Area:** A shorthand of the subject area. See Section 2.12 for a list of these.
  - **Document Section:** Denoted by the four left-hand digits in the schema. For example, the ’03-04’ in PRIV-03-04-01a means section 3.4 of the privacy requirements (set out in **TDIF: 04 - Functional Requirements**).
  - **Requirement:** Denoted by the two right-hand digits in the schema. For example, the ‘01’ in PRIV-03-04-01a means requirement 01 in section 3.4 of the privacy requirements.
  - **Sub-Requirement:** Denoted by a unique letter at the right-hand side of the schema. For example, the ‘a’ in PRIV-03-04-01a means the first sub-requirement linked to requirement 01 in section 3.4 of the privacy requirements.

- **Updated:** The month/year the requirement was last updated.

- **Applicability:** The Accredited Role to whom the requirement applies. The roles include:
  
  - **Attribute Service Providers,** denoted by an ‘A’
  - **Credential Service Providers,** denoted by a ‘C’
  - **Identity Service Providers,** denoted by an ‘I’
  - **Identity Exchanges** denoted by an ‘X’.

- **Requirement text:** The requirement to be met.
2.12 Subject area description

The following table sets out the shorthand descriptions for the TDIF requirements subject areas.

<table>
<thead>
<tr>
<th>TDIF Document</th>
<th>Section</th>
<th>Shorthand</th>
</tr>
</thead>
<tbody>
<tr>
<td>03 Accreditation</td>
<td>All Sections</td>
<td>ACCRED</td>
</tr>
<tr>
<td>Process</td>
<td>2 – Fraud control requirements</td>
<td>FRAUD</td>
</tr>
<tr>
<td></td>
<td>3 – Privacy Requirements</td>
<td>PRIV</td>
</tr>
<tr>
<td></td>
<td>4 – Protective Security Requirements</td>
<td>PROT</td>
</tr>
<tr>
<td></td>
<td>5 – User Experience Requirements</td>
<td>UX</td>
</tr>
<tr>
<td></td>
<td>6 – Technical Testing Requirements</td>
<td>TEST</td>
</tr>
<tr>
<td></td>
<td>7 – Functional Assessments</td>
<td>ASSESS</td>
</tr>
<tr>
<td>04 Functional</td>
<td>2 – Fraud control requirements</td>
<td>FRAUD</td>
</tr>
<tr>
<td>Requirements</td>
<td>3 – Privacy Requirements</td>
<td>PRIV</td>
</tr>
<tr>
<td></td>
<td>4 – Protective Security Requirements</td>
<td>PROT</td>
</tr>
<tr>
<td></td>
<td>5 – User Experience Requirements</td>
<td>UX</td>
</tr>
<tr>
<td></td>
<td>6 – Technical Testing Requirements</td>
<td>TEST</td>
</tr>
<tr>
<td></td>
<td>7 – Functional Assessments</td>
<td>ASSESS</td>
</tr>
<tr>
<td>05 Role Requirements</td>
<td>2 – Common Role Requirements</td>
<td>ROLE</td>
</tr>
<tr>
<td></td>
<td>3 – Identity Service Provider Requirements</td>
<td>IDP</td>
</tr>
<tr>
<td></td>
<td>4 – Credential Service Provider Requirements</td>
<td>CSP</td>
</tr>
<tr>
<td></td>
<td>5 – Attribute Service Provider Requirements</td>
<td>ASP</td>
</tr>
<tr>
<td>06 Federation Onboarding Requirements</td>
<td>All Sections</td>
<td>FED</td>
</tr>
<tr>
<td>06B OpenID Connect 1.0 Profile</td>
<td>All Sections</td>
<td>OIDC</td>
</tr>
<tr>
<td>06C SAML 2.0 Profile</td>
<td>All Sections</td>
<td>SAML</td>
</tr>
<tr>
<td>07 Annual Assessment</td>
<td>All Sections</td>
<td>ANNUAL</td>
</tr>
</tbody>
</table>

2.13 What is not covered in the TDIF

The scope of the TDIF is limited to the accreditation of Applicants and maintenance of Participant’s accreditations (Accredited Participants). There are several items not covered by the TDIF, including:

- Cost or fee schedules for the provision of identity services.
- Liability arrangements for Accredited Participants.
• Details on how to join the *Australian Government’s Identity Federation*.
• Requirements to be met by *Relying Parties* to join the *Australian Government’s Identity Federation*.
• A catalogue of participating services available through the *Australian Government’s Identity Federation*.
• Technical details or other information related to the *Australian Government’s Identity Federation* test environments.
• Operational functions of the *Australian Government’s Identity Federation*.
• Service level agreements.
• Governance arrangements for the *Australian Government’s Identity Federation*. 
References

In developing the TDIF the following sources have been considered¹.

3. *Archives Act 1983* (Cth)
6. Attorney-General’s Department (2011) *Improving the integrity of identity data: recording of a name to establish identity – better practice guidelines for Commonwealth Agencies* [PDF], Australian Government Attorney-General’s Department.

¹ Some sources contain hyperlinks.


38. Crimes Act 1914 (Cth)


50. Disability Discrimination Act 1992 (Cth)


90. OASIS Security Services Technical Committee (2008) Identity Provider Discovery Service Protocol and Profile [IdPDisco] [PDF], OASIS.
91. OASIS Security Services Technical Committee (2009) SAML V2.0 Metadata Extension for Entity Attributes Version 1.0 [MetaAttr] [PDF], OASIS, Cantor S (ed).
92. OASIS Security Services Technical Committee (2019) SAML V2.0 Metadata Interoperability Profile Version 1.0 [SAML2MDIOP] [PDF], OASIS, Cantor S (ed).
93. OASIS Security Services Technical Committee (2011), Metadata Profile for Algorithm Support Version 1.0 [SAML2MetaAlgSup] [PDF], OASIS, Cantor S (ed).
95. OASIS Security Services Technical Committee (2012) SAML Version 2.0 Errata 05 [SAML2Errata] [PSF], OASIS, Cantor S (ed).
96. OASIS Security Services Technical Committee (2012) SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0 [MetaUI], OASIS, Cantor S (ed).
102. Privacy Act 1988 (Cth)
103. Proceeds of Crime Act 2002 (Cth)
104. Proceeds of Crime Regulations 2002 (Cth)
105. Public Governance, Performance and Accountability Act 2013 (Cth)
106. Public Governance, Performance and Accountability Rule 2014 (Cth)
107. Public Service Act 1999 (Cth)
114. United Kingdom Cabinet Office (2012) Good Practice Guide - Requirements for secure delivery of online public services (GPG 43), United Kingdom Cabinet Office, Gov.UK.