SMB1001 Certification Practice Statement (CPS)

Version 1.0
3 September 2024

COPYRIGHT PROTECTED DOCUMENT

Email: support@cybercert.com.au
Web: www.cybercert.com.au

Patents pending: 2023903514, 2023903509, 2023903507, 2023903506.

Published in Australia

Document Control

Preparation

Role	Description
Authorised by:	Peter Maynard
Document owner:	CyberCert Certification Registrar
Author:	Dr David Ross, Dr Ryan Ko, Peter Maynard
Issue date:	01 September 2024
Next review date:	November 2024
Source file location:	https://cybercert.com.au/SMB1001-CPS.pdf

Document History

Version	Date	Section	Nature of amendment	Author
1.0	01/11/2023	All	Initial issue	Peter Maynard
1.0	03/09/2024	All	Change to SMB1001	Elinor Tsen

Table of Contents

1. Introduction

This is a public document. It may be sourced by any party that relies on (**Relying Party**) a certificate issued by CyberCert against the Cyber Security Certification Australia (**CSCAU**) Standard *SMB1001 — Multi-tiered cyber security certification standard for small and medium-sized businesses* (***CSCAU SMB1001***).

The purpose of this *CyberCert SMB1001 Certification Practice Statement* (**CPS**) is to describe the practices employed by CyberCert and outlines the responsibilities of the involved parties when issuing, recertifying and managing CyberCert certificates for the *CSCAU SMB1001* standard.

The procedures in this Certification Practice Statement have been developed to support the *CyberCert Certification Policy*. The *CyberCert Certification Policy* is not required by Relying Parties and is not a public document. This CPS provides all the information Relying Parties require to understand CyberCert's practices in certification activities against *CSCAU SMB1001*.

1.1 Overview

1.1.1 CSCAU is an Australian standards development company that facilitates industry-led cyber security certification standards, focusing on dynamic standards for small and medium-sized businesses.

1.1.2 CyberCert is a global Conformity Assessment Body (**CAB**) based in Australia.

1.1.3 CyberCert is accredited to assess conformance against particular CSCAU standards.

1.1.4 CyberCert is accredited to assess conformance against CSCAU standard *SMB1001 — Multi-tiered cyber security certification standard for small and medium-sized businesses* (***CSCAU SMB1001***) for Levels 1 through 3.

1.1.5 *CSCAU SMB1001* is a CSCAU multi-level cyber security certification dynamic standard for small and medium-sized businesses. *Note: SMB1001 is reviewed and updated annually to keep pace with controls fit for the latest cyber threat environments. This CPS describes the practices employed by CyberCert when issuing, recertifying and managing CyberCert certificates specifically for the CSCAU SMB1001 version of the standard. For certificates issued against other versions of the standard, please refer to the CPS for that particular version.*

1.1.6 Certification is available in any one of five levels of validation and attestation, from Level 1 (minimum requirements of the standard and minimal independent validation) to Level 5 (all requirements of the standard and all assertions independently validated).

1.1.7 CyberCert issues SMB1001 certificates for a number of different levels of attestation. Only the practices listed in this CPS for a particular level of attestation are performed by CyberCert in issuing the particular SMB1001 certificate. Relying Parties should carefully consider the practices listed in this document that have been performed by CyberCert for a particular level of attestation, before relying on the certification.

1.1.8 This CPS describes:

- Participants
- How certificates are issued, recertified and managed
- Security (personnel, audit, etc.)
- Audit procedures
- Business and legal issues

1.2 Document control

1.2.1 Document name and identification

1.2.1.1 The name of this document is the “CyberCert SMB1001 Certification Practice Statement (CPS)”.

1.2.1.2 The current version of this document is available from CyberCert.

1.2.1.3 The document history is maintained following the cover page so Relying Parties can assess changes relevant for existing certificates.

1.2.2 Scope

1.2.2.1 This Certification Practice Statement encompasses all CyberCert certification operations and activities against *CSCAU SMB1001*, including all assessments and validation, in all business units at all sites, whether on-premises, on-line, or via external parties, including staff engaged in any form of remote working.

1.2.3 Application

1.2.3.1 The *CyberCert Certification Policy* binds all CyberCert staff and all CyberCert certification clients to the procedures detailed in this Certification Practice Statement.

1.2.3.2 This Certification Practice Statement applies to all CyberCert staff — regardless of role, including agency workers, trainees on vocational or work experience schemes, and volunteers — and all CyberCert clients seeking or recertifying a CyberCert certification; and any and all Relying Parties choosing to rely on a CyberCert certification.

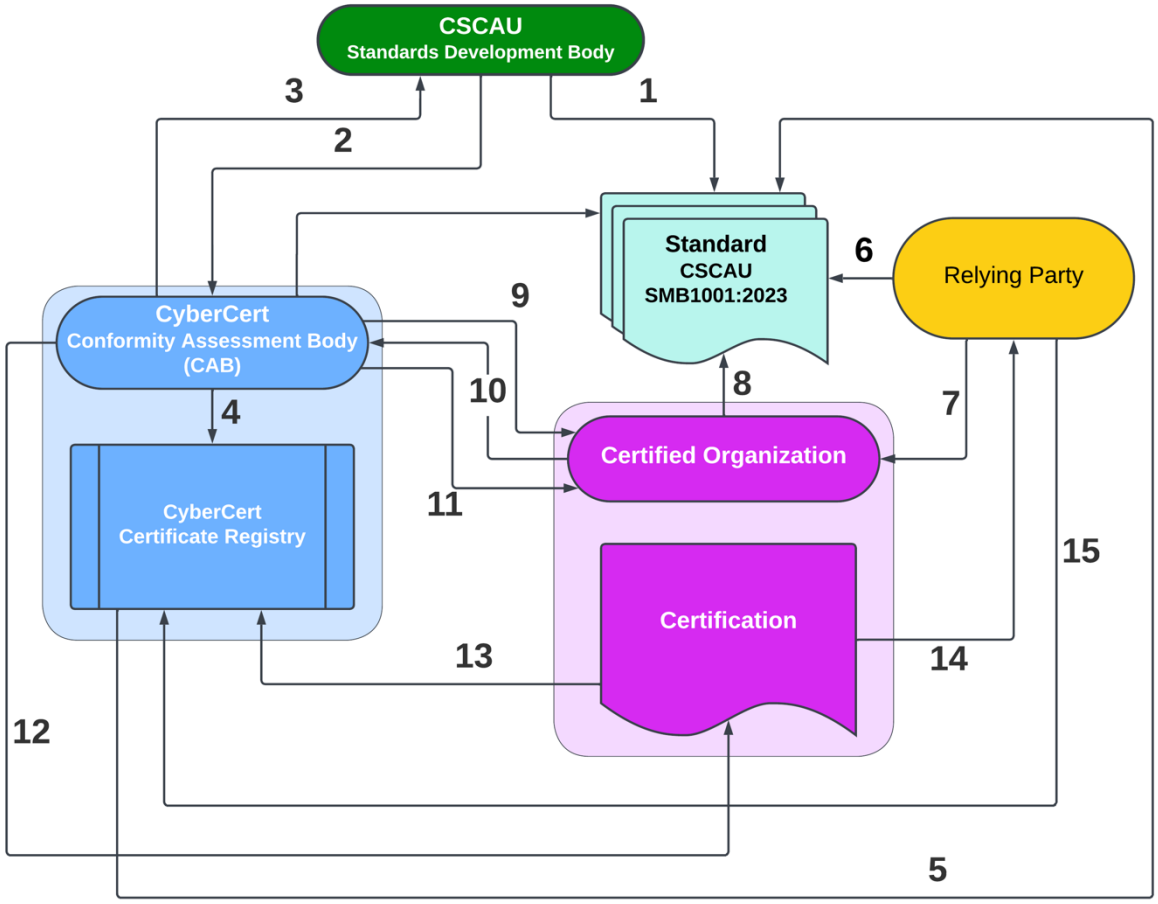
1.2.3.3 Relying Parties MUST NOT infer that any practices not listed in this document, for a particular level of attestation, have been performed by CyberCert.

1.3 CSCAU SMB1001 certification participants

1.3.1 Summary

1.3.1.1 The certification participants consist of an independent standards development body, an accreditation body, one or more Conformity Assessment Bodies (CABs) involved in the assessment and issuing of certificates, the certificate Subscribers and the Relying Parties. A visual overview is provided in

1.3.1.2 Figure *1*.



Contents

1. **CSCAU** develops and maintains the **Standard**
2. **CSCAU** accredits CABs to certify **organizations**
3. **CyberCert** delivers report on certification activities to **CSCAU**
4. **CyberCert** maintains **CyberCert Certificate Registry**
5. **CyberCert** maintains accreditation to certify against the **Standard**
6. **Relying Party** requires organizations to comply with the **Standard**
7. **Relying Party** does business with **Certified Organization**
8. **Certified Organization** attests to meeting requirements for the **Standard**
9. **CyberCert** delivers subscriber agreement to **Certified Organization**
10. **Certified Organization** makes attestation to **CyberCert**
11. **CyberCert** validates details for **Certified Organization**
12. **CyberCert** issues certificate to **Certified Organization**
13. **Certificate** details are recorded in **CyberCert Certificate Registry**
14. **Relying Party** relies on **CyberCert Certification**
15. **Relying Party** can validate Certificate using **CyberCert Certificate Registry**

Figure 1: Standards Conformity, Governance and Certification Stakeholders

1.3.2 Standards development body

1.3.2.1 Cyber Security Certification Australia (CSCAU) is an independent standards development body. It consists of an executive body managing the development of standards and other instruments by various Steering Committees; and an independent Standards and Certification Oversight Board (SCOB) — an independent skill-based board comprised of authorities in their fields — separate to the executive body, responsible for review and to ensure quality of outputs from the executive body's Steering Committees.

1.3.3 Accreditation body

1.3.3.1 The default accreditation body shall be the standards development body, Cyber Security Certification Australia (CSCAU).

1.3.3.2 The accreditation body accredits Conformity Assessment Bodies (CABs) to assess their Subscribers' conformance to the *CSCAU SMB1001 — Multi-tiered cyber security certification for SMBs* standard.

1.3.3.3 For new standards that do not yet have an approved Accreditation Scheme, the accreditation body is the standards development body, Cyber Security Certification Australia (CSCAU).

1.3.3.4 Once an approved Accreditation Scheme for *CSCAU SMB1001 — Multi-tiered cyber security certification for small and medium-sized businesses* has been developed, the accreditation body shall be JAS-ANZ or other relevant Mutual Recognition Arrangements (MRAs).

1.3.4 Conformity Assessment Bodies (CABs)

1.3.4.1 Conformity Assessment Bodies (CABs) are the entities that assess their Subscribers' conformance to the *CSCAU SMB1001* standard, and subsequently generate and issue SMB1001 certificates.

1.3.4.2 CABs are accredited by the accreditation body to assess their Subscribers' conformance to the *CSCAU SMB1001* standard.

1.3.4.3 CyberCert is an Australian CAB accredited by CSCAU to assess clients' conformance to the *CSCAU SMB1001* standard.

1.3.4.4 Each CAB has a single Certification Manager (CM) who is responsible for overseeing the management and operation of all certification components of their respective CAB.

1.3.4.5 Each CAB has one or more Authorising Officers (AO) who are responsible for approving the issuing of certificates.

1.3.4.6 Each CAB has one or more Certifying Officers (CO) who are responsible for issuing certificates.

1.3.4.7 For Level 1, 2, and 3 certifications, the roles of CM, AO and CO may be performed by a single combined role of a Certification Registrar (CR).

1.3.4.8 Level 4 and 5 certifications require separation of duties between the AO and CO roles and, as such, the roles of the AO and CO must be performed by two separate individuals.

1.3.4.9 In all cases, the roles of the CM and the AO may be performed by the same person.

1.3.4.10 CyberCert operates a register that holds issued certificates.

1.3.4.11 Each CAB has one or more Auditors who are responsible for overseeing the audit and compliance of components of the CAB.

1.3.5 Subscribers

1.3.5.1 Entities or individuals applying for, or named in, a certificate issued by a CAB are Subscribers.

1.3.5.2 All Subscribers for certificates issued under any CPS must formally agree to be bound by the terms of a Subscriber Agreement that includes, at least, acknowledgement and acceptance of all the provisions of Clause 9 of this CPS, before the Subscriber is issued with a certificate. The Subscriber Agreement may be concluded online. CABs shall enforce the use of Subscriber Agreements in accordance with this clause.

1.3.5.3 The obligations contained in this CPS must be agreed to by any party requesting certificates under this CPS.

1.3.6 Relying Parties

1.3.6.1 Entities or individuals that act in reliance on certificates issued under *CSCAU SMB1001* are Relying Parties. Relying Parties may or may not be Subscribers.

1.3.6.2 The Relying Parties rely on the certificate to the stated level of certification assurance.

1.3.6.3 A Relying Party should ensure it is satisfied, with due diligence, that the level of certification assurance asserted in a SMB1001 certificate is suitable for their application.

1.3.6.4 No party is obligated to rely on any certificate, however a Relying Party that chooses to rely on a SMB1001 certificate, in doing so, must agree to be bound by the obligations contained in this CPS.

1.3.7 Other participants

1.3.7.1 Besides the auditor roles and functions of the various authorities, from time-to-time external third-party auditor entities may be engaged to meet and verify the compliance provisions of the CSCAU SMB1001.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

1.4.1.1 The certificates issued under this CPS are for validation of a particular level of attestation in claims of Subscribers on their conformance to the *CSCAU SMB1001* standard.

1.4.1.2 Subscribers may present their certificates to Relying Parties, in accordance with the terms of their Subscriber Agreement and the provisions of Clause 9 of this CPS, as validation, of a particular level of attestation, on their claims of conformance to the *CSCAU SMB1001* standard.

1.4.1.3 Subscribers may publicly advertise their certificates to potential Relying Parties, in accordance with the terms of their Subscriber Agreement and the provisions of Clause 9 of this CPS, as validation, of a particular level of attestation, on their claims of conformance to the *CSCAU SMB1001* standard.

1.4.1.4 Relying Parties MAY rely on the certificate to the stated level of certification assurance.

1.4.1.5 A Relying Party SHOULD ensure it is satisfied, with due diligence, that the level of certification assurance asserted in a SMB1001 certificate is suitable for their application.

1.4.1.6 Additional uses of the certificates, consistent with the basic goals cited above, are also permitted.

1.4.2 Prohibited certificate uses

1.4.2.1 Any uses other than those described in Section 1.4.1 are prohibited.

1.5 Policy administration

1.5.1 Organization administering the document

1.5.1.1 This CPS is administered by CyberCert.

1.5.2 Contact person

1.5.2.1 The CyberCert CPS point of contact is the Certification Registrar. The online point of contact is available via the Help contact located on the CyberCert landing page at https://cybercert.au The postal address for the point of contact is GPO Box 1515, Brisbane, Australia.

1.5.3 CPS approval procedures

1.5.3.1 CyberCert may amend the terms of this CPS from time to time. When this happens, the new version of the CPS will be posted to CyberCert's website, and the CPS URL (https://cybercert.com.au/SMB1001-CPS.pdf) will be updated to point to the new version of the CPS.

1.6 Definitions

1.6.1 **Audit System Administrator** – A System Administrator (see below) for computer systems involved with audit functions, including audit trails of the System Administrators of other production systems. Audit System Administrators have no duties on, and no access to, other production systems. Other production System Administrators have no duties on, and no access to, computer systems involved with audit functions.

1.6.2 **Australian Business Number (ABN)** – A unique 11-digit identifier issued by the Registrar of the Australian Business Registry Services to every entity carrying on or starting an enterprise in Australia or making supplies connected with the indirect tax zone, including every Corporations Act company.

1.6.3 **Australian Business Register (ABR)** – An Australian a comprehensive national business dataset whose registrar is also the Registrar of the Australian Business Registry Services and the Commissioner of Taxation.

1.6.4 **Australian Company Number (ACN)** – A unique nine-digit identifier issued by the Australian Securities and Investments Commission (ASIC) to every company registered under Australia's *Corporations Act 2001 (Cth)*.

1.6.5 **Australian Securities and Investments Commission (ASIC)** – An independent Australian Government body under the *Australian Securities and Investments Commission Act 2001 (Cth)* responsible for regulating Australian corporations registered under Australia's *Corporations Act 2001 (Cth)*, financial services and consumer credit, and authorised financial markets.

1.6.6 **Authentication** – The process of verifying the claimed identity of an entity.

1.6.7 **Authorising Officer (AO)** – The role of one or more (named) people in a Conformity Assessment Body (CAB) who are responsible for approving the issuing of certificates.

1.6.8 **Certification Manager (CM)** – The role of a single (named) person in each Conformity Assessment Body (CAB) who is responsible for overseeing the management and operation of all certification components of their CAB.

1.6.9 **Certification Practice Statement (CPS)** – A CPS is a document that specifies the practices that a CAB employs in issuing certificates.

1.6.10 **Certification Registrar (CR)** – The role of one or more (named) people in a Conformity Assessment Body (CAB) who oversee the currency and accuracy of the Registry,and are responsible for a combination of some or all of AO, CO, and CM roles.

1.6.11 **Certifying Officer (CO)** – The role of one or more (named) people in a Conformity Assessment Body (CAB) who are responsible for issuing certificates.

1.6.12 **Conformity Assessment Body (CAB)** – A CAB is an accredited authority that assesses conformance issues and manages SMB1001 certificates.

1.6.13 **Evidence Of Identity (EOI)** – The process implemented to determine the identity of an entity using documents or other information identifying the entity. The *Financial Transactions Reports Act 1988 (Cth)* establishes document categories for EOI (Primary Identification Documents and Secondary Identification Documents). See https://www.austrac.gov.au/business/legislation/financial-transaction-reports-act. (Current version at time of writing: https://www.legislation.gov.au/Details/C2018C00115)

1.6.14 **Force Majeure** – A Force Majeure event means any occurrence or omission that is beyond the reasonable control of a party that prevents or delays that party from performing any of its obligations under this CPS, policy or Subscriber Agreement.

1.6.15 **Identification** – The process of establishing the identity of an entity. Identification does not necessarily include authentication of that identity. Typically, both identification and authentication will be required for most certification circumstances.

1.6.16 **Identification Document** – means a Primary Identification Document or a Secondary Identification Document.

1.6.17 **Participant** – An individual or organization that plays a role as a Subscriber, Relying Party, CAB, register service provider, or similar entity.

1.6.18 **Personal Information (PI)** – has the meaning given by Section 6 of the *Privacy Act 1988 (Cth)*: information or an opinion about an identified individual, or an individual who is reasonably identifiable.

1.6.19 **Primary Identification Document** – has the meaning given by Section 3 of the *Financial Transactions Reports Act 1988 (Cth)*, in relation to a person, in a particular name, means: (a) a certified copy, or an extract, of a birth certificate of the person; or (b) a certified copy of a citizenship certificate of the person; or (c) an international travel document for the person; or (d) any other prescribed document; that shows that name as the person's name. See https://www.austrac.gov.au/business/legislation/financial-transaction-reports-act. (Current version at time of writing: https://www.legislation.gov.au/Details/C2018C00115)

1.6.20 **Register** – The on-line storage area where the Conformity Assessment Body (CAB) stores issued certificates.

1.6.21 **Relying Party** – A recipient of a certificate who acts in reliance on that certificate.

1.6.22 **Secondary Identification Document** – has the meaning given by Section 3 of the *Financial Transactions Reports Act 1988 (Cth)*, in relation to a person, in a particular name, means a document (other than a primary identification document) which establishes the identity of the person in that name. See https://www.austrac.gov.au/business/legislation/financial-transaction-reports-act. (Current version at time of writing: https://www.legislation.gov.au/Details/C2018C00115)

1.6.23 **SMB1001 Level [1-5] certificate** – A certificate issued by a CAB attesting to a particular level, from "Level 1" to "Level 5" of validation as described in this CPS, of that same level of attestation, from "Level 1" to "Level 5" as described in the *CSCAU SMB1001* standard of the named certificate subject's conformance with the requirements of that same level, from "Level 1 Requirements" to "Level 5 Requirements" in the *CSCAU SMB1001* standard.

1.6.24 **Subscriber** – A subject of a certificate to whom a certificate is issued.

1.6.25 **Subscriber Agreement** – An agreement between a CAB and a Subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.

1.6.26 **System Administrator** – A privileged computer system user with the ability to configure or modify components of a computer system beyond the abilities of a standard user.

1.6.27 **Validation** – The process of identifying and verifying conformity details.

1.7 Initialisations and Acronyms

1.7.1 **ABN** – Australian Business Number

1.7.2 **ABR** – Australian Business Register

1.7.3 **ABRN** – Australian Registered Body Number

1.7.4 **ACN** – Australian Company Number

1.7.5 **AO** – Authorising Officer

1.7.6 **ASIC** – Australian Securities and Investments Commission

1.7.7 **CAB** – Conformity Assessment Body

1.7.8 **CM** – Certification Manager

1.7.9 **CO** – Certifying Officer

1.7.10 **CPS** – Certification Practice Statement

1.7.11 **PI** – Personal Information

1.7.12 **UTC** – official abbreviation in all languages for the English “Coordinated Universal Time” (in French UTC is “Temps Universel Coordonné”; in German “Koordinierte Weltzeit”)

2. Publication and Registry Responsibilities

2.1 Registers

2.1.1 CyberCert maintains a local register of all certificates issued by CyberCert.

2.1.2 The register SHALL include the following information

- Organization Name of Subscriber;
- Date certification issued;
- Certification ID;
- Contact email and/or phone number for individual officer of Subscriber;
- Name of officer from the Subscriber;
- Name of attesting office from the Subscriber;
- Certification completed;
- Level of certification completed;
- Version / Release of the standard attested to.

2.1.3 The CyberCert local certificate registry generates immutable audit trails of register activity.

2.2 Publication of certification information

2.2.1 CyberCert uploads certificates issued by CyberCert to a local certificate registry accessible via https://registry.cybercert.app

2.2.2 CyberCert SHALL share the registry with CSCAU as required by this CPS or any relevant policy.

2.3 Time or frequency of publication

2.3.1 Certificates will be published within one working day after issuance.

2.4 Access controls on registers

2.4.1 Read access to CyberCert's local certificate registry is public.

2.4.2 Write access to CyberCert's local certificate registry is restricted to CyberCert COs and the CyberCert CM.

2.4.3 Procedural controls separate the duties of CyberCert AOs and CyberCert COs. For SMB1001 Level 4 and Level 5 certification, a certificate cannot be issued by a CyberCert CO without a successful audit by a CyberCert AO, however a CyberCert AO cannot issue certificates themselves.

2.4.4 CyberCert AOs do not have write access to CyberCert's local certificate registry.

2.4.5 Computer System Administrators and other privileged users of CyberCert's local certificate registry have all activity logged with immediate duplication to a central audit log controlled by separate Audit System Administrators.

2.4.6 Computer System Administrators and other privileged users of CyberCert's local certificate registry have no duties on, and no access to, computer systems involved with audit functions. Audit System Administrators have no duties on, and no access to, CyberCert's local certificate registry.

3. Identification and Authentication

3.1 Naming

3.1.1 The Subject of each certificate issued by CyberCert is identified by their registered name as listed in the Australian Business Register (ABR) and, their ABN OR ARBN.

3.1.2 Certificates SHALL only be issued to businesses using their registered name as listed in the ABR. There is currently no provision to add trading names or other names to the registered name obtained from the ABR.

3.1.3 Certificates SHALL NOT be issued anonymously or pseudonymously.

3.1.4 Certificate subject names SHALL be unique within the scope of the ABR.

3.1.5 Certificate subject names MAY include trademarks or service marks where these form all or part of the registered name as listed in the ABR, however any such trademarks or service marks SHALL NOT be identified as such. The certificate subject name SHALL appear exactly as listed in the ABR.

3.1.6 For a foreign business not registered in Australia, either as an Australian business, Registrable Australian body or registered foreign business, the Subject of each certificate issued by CyberCert is identified by their registered name in the country that they are registered and their company identification number.

3.2 Initial Identity validation

3.2.1 Method to set organization name

3.2.1.1 Subscribers must supply their ABN OR ABRN at time of initial registration.

3.2.1.2 CyberCert validates the Subscriber's supplied ABN OR ABRN in the Australian Business Register (ABR) and records their registered entity name.

3.2.1.3 CyberCert uses only the Subscriber's registered entity name in the preparation of all business documents, the Subscriber Agreement and the Subject name of any certificate subsequently issued by CyberCert.

3.2.1.4 For a foreign business not registered in Australia, either as an Australian business, Registrable Australian body or registered foreign business, Subscribers must contact CyberCert and provide information for identification purposes (see Section 3.2.3).

3.2.2 Authentication of organization identity

3.2.2.1 CyberCert obtains approved Subscriber ABNs from CyberCert clients and partners.

3.2.2.2 Organizations CANNOT initiate certification until their ABN has been supplied by a CyberCert client or a CyberCert partner.

3.2.2.3 CyberCert validates the Subscriber's supplied ABN in the Australian Business Register (ABR).

3.2.3 Authentication of individual identity

3.2.3.1 CyberCert has existing business relationships with its clients and partners.

3.2.3.2 New clients must establish a business relationship with CyberCert before they can conduct business with CyberCert.

3.2.3.3 Individual officers of Subscribers are NOT authenticated in order to request certification.

3.2.3.4 Individual officers of Subscribers are NOT authenticated to request re-certification.

3.2.3.5 Individual officers of Subscribers SHALL be authenticated to request modification.

3.2.3.6 Individual officers of Subscribers SHALL be authenticated to request revocation.

3.2.3.7 CyberCert validates individuals requesting modification or revocation of a certificate by: a CyberCert AO or a CyberCert CO or the CyberCert CM sighting, either in person or via live video link, at least one Primary Identification Document or at least two Secondary Identification Documents.

3.2.3.8 The CyberCert officer validating the individual SHALL record the fact that authentication has occurred, but SHALL NOT record any of the authentication data provided.

3.2.3.9 No personal information (PI) shall be collected or stored, except for the individual's name, role, and any contact information relevant to the certification process.

3.2.3.10 The CyberCert officer validating the individual SHALL record their own name and role, the name of the individual being identified, the nature of the Evidence Of Identity (EOI) sighted (passport with issuing country, drivers licence with issuing state, etc.) and the date on which they validated the individual's identity.

3.2.3.11 The CyberCert officer validating the individual SHALL NOT record the actual EOI, nor any number, code, or other additional detail from the EOI.

3.2.4 Method and authentication for foreign businesses

3.2.4.1 A Subscriber that is a foreign business not registered in Australia MUST provide CyberCert with the following information:

- Full name of foreign company;
- Country of incorporation OR registration;
- Name of foreign body that registered the business;
- Company Identification Number;
- Registered Address of business;
- Business type – private, public listed, majority owned subsidiary of an Australian public listed company OR regulated in Australia;
- Directors

3.2.4.2 CyberCert SHALL verify the information provided by searching the relevant foreign registration bodies

3.2.4.3 If verification is not achievable, CyberCert MAY request a certified copy of the certificate issued by the relevant foreign registration body OR a disclosure certificate given by an individual acting as agent of the business.

3.2.5 Non-verified Subscriber information

3.2.5.1 No non-verified Subscriber data is included in certificates issued under this CPS.

3.2.6 Validation of authority

3.2.6.1 Requests for certification may only be made by a person identified as an executive office, owner OR senior executive of the Subscriber.

3.2.6.2 CyberCert shall require an executive officer, owner OR senior executive of the Subscriber to be identified and authenticated in accordance with Clause 3.2.3 of this CPS.

3.2.6.3 Subscribers are responsible for notifying CyberCert when existing authorised officers of the Subscriber are no longer authorised to act on behalf of the Subscriber.

3.2.7 Criteria for interoperation

3.2.7.1 CyberCert is an Australian CAB accredited by CSCAU to assess clients' conformance to the Requirements of the *CSCAU SMB1001 — Multi-tiered cyber security certification for small and medium-sized businesses*. CyberCert SMB1001 certifications are fully compatible with any other SMB1001 certifications by any CAB accredited by CSCAU.

3.3 Identification and authentication for recertification

3.3.1 Identification and authentication for routine recertification

3.3.1.1 Subscribers' current (not expired) CyberCert certifications are sufficient for both identification and authentication, for recertification.

3.3.1.2 Recertification of a non-CyberCert certification shall be processed as a new certification, with identification and authentication in accordance with Clause 3.2 of this CPS.

3.3.1.3 CyberCert validates the Subscriber's ABN in the Australian Business Register (ABR) and records any changes to their registered entity name.

3.3.1.4 Existing validated individual executive officers, owners OR senior executives of the Subscriber are not re-validated.

3.3.1.5 Subscribers are responsible for notifying CyberCert when existing authorised officers of the Subscriber are no longer authorised to act on behalf of the Subscriber.

3.3.1.6 New or additional individual executive officers, owners OR senior executives of the Subscriber are validated in accordance with Clause 3.2.3 of this CPS.

3.3.2 Identification and authentication for recertification after expiry

3.3.2.1 An expired certification is NOT sufficient for either identification or authentication, and identification and authentication for recertification of an expired certification

shall be processed as a new certification in accordance with Clause 3.2 of this CPS, in its entirety.

3.3.2.2 While individual identities of executive officers, owners OR senior executives do not need to be re-validated, the roles of those officers as executive officers, owners OR senior executives of the Subscriber shall be re-validated.

3.4 Identification and authentication for modification

3.4.1 Identification and authentication for correction of error

3.4.1.1 Subscribers' current (not expired) CyberCert certifications are sufficient for both identification and authentication, for correcting a CyberCert error (not a change) in a certificate Subject name, certification level, or relevant date.

3.4.1.2 An expired certification is not valid and no historic corrections shall be considered.

3.4.2 Identification and authentication for change of registered name

3.4.2.1 Subscribers' current (not expired) CyberCert certifications are sufficient for both identification and authentication, for changing the Subject name to match a new registered name as listed in the ABR, for the same ABN.

3.4.2.2 An expired certification is NOT sufficient for either identification or authentication, and identification and authentication for any change to an expired certification shall be processed as a new certification in accordance with Clause 3.2 of this CPS, in its entirety.

3.4.2.3 While individual identities of executive officers, owners OR senior executives do not need to be re-validated, the roles of those officers as executive officers, owners OR senior executives of the Subscriber SHALL be re-validated.

3.4.3 Identification and authentication for change of ABN/ACN

3.4.3.1 A change of ABN shall be processed as a new certification, and identification and authentication shall be processed as for a new certification in accordance with Clause 3.2 of this CPS, in its entirety.

3.4.4 Identification and authentication for change of certification level

3.4.4.1 Subscribers' current (not expired) CyberCert certifications are sufficient for identification ONLY, for the certification process at any other level.

3.4.4.2 Subscribers' current (not expired) CyberCert certifications are sufficient for both identification and authentication, for the certification process at the SAME level or any LOWER level.

3.4.4.3 Subscribers' current (not expired) CyberCert certifications are NOT necessarily sufficient for authentication at a higher level of certification. For certifications at a higher level, refer to the relevant clause for identification and authentication for "recertification" at that higher level.

3.4.5 Identification and authentication for change of relevant dates

3.4.5.1 Any change of dates shall be processed as a recertification, with identification and authentication processed in accordance with Clause 3.3 of this CPS.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who can submit a certification application

4.1.1.1 Requests for certification may only be made by a person identified as an officer, owner, senior executive or nominee of the Subscriber. See Clause 3.2.6 of this CPS.

4.1.2 Enrolment process and responsibilities

4.1.2.1 An officer for the Subscriber requests a CyberCert account for a particular ABN.

4.1.2.2 The CyberCert account holder can then register in the CyberCert registration system at https://cybercert.au/register and be linked to the associated CyberCert account.

4.1.2.3 Once registered, the CyberCert account holder MAY carry out a *CSCAU SMB1001 — Multi-tiered cyber security certification for small and medium-sized businesses* request via https://cybercert.au/.

4.1.2.4 The Subscriber's representative first provides their responses to a series of questions to provide an initial assessment of the Subscriber's conformance to the *CSCAU SMB1001 — Multi-tiered cyber security certification for small and medium-sized businesses* requirements.

4.1.2.5 The CyberCert registration system will then offer to proceed with an appropriate level of attestation to the *CSCAU SMB1001 — Multi-tiered cyber security certification for small and medium-sized businesses* requirements.

4.1.2.6 The Subscriber's representative then requests to proceed with a certification, providing their attestation for the requested level of the *CSCAU SMB1001 — Multi-tiered cyber security certification for small and medium-sized businesses* requirements.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

4.2.1.1 Subscribers must supply their ABN at time of initial registration.

4.2.1.2 The registration process shall validate the ABN and display the registered name as listed in the Australian Business Register (ABR).

4.2.1.3 The Subscriber must accept the name as presented or provide a different ABN.

4.2.1.4 The Subscriber must then create or provide their CyberCert account credentials.

4.2.2 Approval or rejection of certificate applications

4.2.2.1 A CyberCert account holder (to be Subscriber) requests a certification, providing their attestation for the requested level of the *CSCAU SMB1001 — Multi-tiered cyber security certification for small and medium-sized businesses* requirements.

4.2.2.2 Through CyberCert's system, the certificate approval/rejection/pending is communicated to the Subscriber.

4.2.3 Time to process certificate applications

4.2.3.1 CyberCert expects to issue a certificate attesting to a certification within 1 business day after approval.

4.2.3.2 A Subscriber has twelve (12) months to complete a certification from the date of purchase of the Subscription as outlined in the User Terms. If the certification has not been completed within the twelve (12) month period the Subscription will expire.

4.3 Certificate issuance

4.3.1 CAB actions during certificate issuance

4.3.1.1 Certificate issuance is handled by CyberCert's internal systems.

4.3.2 Notification to Subscriber by the CAB of issuance of certificate

4.3.2.1 The Subscriber is notified of the issuance of the initial certificate by way of the CyberCert registration system at https://cybercert.au/ and via email to the address provided during the attestation process.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

4.4.1.1 A Subscriber is deemed to have accepted a certificate issued by CyberCert unless the Subscriber explicitly requests modification of the certificate using the procedures described in Section 4.7 of this CPS.

4.4.2 Publication of the certificate by CyberCert

4.4.2.1 Certificates will be published at the registers described in Clause 2.1 of this CPS once issued, following the conduct described in Section 4.4.1. This will be done within 1 business day.

4.4.3 Notification of certificate issuance by the CAB to other entities

4.4.3.1 By registering the newly certified Subscriber into the publicly-accessible registry, CyberCert implicitly notifies all *CSCAU SMB1001 — Multi-tiered cyber security certification for small and medium-sized businesses* Relying Parties when a certificate is published.

4.5 Certificate usage

4.5.1 Subscriber certificate usage

4.5.1.1 The certificates issued under this CPS are for validation of a particular level of attestation in claims of Subscribers on their conformance to the *CSCAU SMB1001* standard.

4.5.1.2 Subscribers may present their issued and valid certificates to Relying Parties, in accordance with the terms of their Subscriber Agreement and the provisions of

Clause 9 of this CPS, as validation, of a particular level of attestation, on their claims of conformance to the *CSCAU SMB1001* standard.

4.5.1.3 Subscribers may publicly advertise their issued and valid certificates to potential Relying Parties, in accordance with the terms of their Subscriber Agreement and the provisions of Clause 9 of this CPS, as validation, of a particular level of attestation, on their claims of conformance to the *CSCAU SMB1001* standard.

4.5.1.4 Additional uses of the valid certificates, consistent with the basic goals cited above, are also permitted.

4.5.1.5 Expired certificates are not permitted to be used.

4.5.2 Relying Party certificate usage

4.5.2.1 The certificates issued under this CPS are for validation of a particular level of attestation in claims of Subscribers on their conformance to the *CSCAU SMB1001* standard.

4.5.2.2 Relying Parties MAY rely on the valid certificate to the stated level of certification assurance.

4.5.2.3 A Relying Party SHOULD ensure it is satisfied, with due diligence, that the level of certification assurance asserted in a SMB1001 certificate is suitable for their application.

4.5.2.4 It is the responsibility of a Relying Party to verify that certificates provided by Subscribers are not expired.

4.6 Certificate recertification

4.6.1 Circumstance for certificate

4.6.1.1 CyberCert will notify the Subscriber at least 3 months in advance of the expiration date.

4.6.1.2 Issued certificates are not renewable.

4.6.2 Who may request recertification

4.6.2.1 Requests for certificate recertification may only be made by a person identified as an executive officer, owner, senior executive OR nominee of the Subscriber. See Clause 3.2.6 of this CPS.

4.6.3 Processing certificate recertification requests

4.6.3.1 A Subscriber requests certificate recertification via the CyberCert registration system at https://cybercert.au/register.

4.6.3.2 Recertification of a non-CyberCert certification shall be processed as a new certification, in accordance with Clauses 4.1, 4.2, and 4.3 of this CPS.

4.6.3.3 Certificate approval/rejection/pending is communicated to the Subscriber.

4.6.4 Notification of new certificate issuance to Subscriber

4.6.4.1 The Subscriber is notified of the issuance of the new certificate by way of the CyberCert registration system at https://cybercert.au/ and via email to the address provided during the attestation process.

4.6.5 Conduct constituting certificate acceptance

4.6.5.1 A Subscriber is deemed to have accepted a certificate issued by CyberCert unless the Subscriber explicitly requests modification of the certificate using the procedures described in Section 4.7 of this CPS.

4.6.6 Publication of the recertified certificate by CyberCert

4.6.6.1 Certificates will be published at the registers described in Clause 2.1 of this CPS once issued, following the conduct described in Section 4.6.5. This will be done within 1 business day.

4.6.7 Notification of certificate issuance by the CAB to other entities

4.6.7.1 By registering the recertified and newly certified Subscriber into the publicly-accessible registry, CyberCert implicitly notifies all *CSCAU SMB1001 — Multi-tiered cyber security certification for small and medium-sized businesses* Relying Parties when a certificate is published.

4.7 Certificate modification

4.7.1 Circumstance for certificate modification

4.7.1.1 A Subscriber may request certificate modification for correcting a CyberCert error (not a change) in a certificate Subject name, certification level, or relevant date.

4.7.1.2 A Subscriber may request certificate modification for changing the Subject name to match a new registered name as listed in the ABR, for the same ABN.

4.7.1.3 A change of ABN shall be processed as a new certification in accordance with Clause 4.1 of this CPS, in its entirety.

4.7.1.4 A change of certification level, other than due a CyberCert error, shall be processed as a new certification in accordance with Clauses 4.1, 4.2, and 4.3 of this CPS.

4.7.1.5 Any change of dates shall be processed as a recertification in accordance with Clause 4.6 of this CPS.

4.7.2 Who may request certificate modification

4.7.2.1 The Subscriber or CyberCert may initiate the certificate modification process.

4.7.2.2 Only individuals who have the appropriate authorisation, per earlier registration of account details, may request modification.

4.7.3 Processing certificate modification requests

4.7.3.1 A Subscriber requests modification by contacting the CyberCert helpdesk via the Help system located on the platform at https://cybercert.au.

4.7.4 Notification of modified certificate issuance to Subscriber

4.7.4.1 A Subscriber is notified of the issuance of a modified certificate by the CyberCert platform.

4.7.5 Conduct constituting modified certificate acceptance

4.7.5.1 A Subscriber is deemed to have accepted a certificate issued by CyberCert unless the subscriber explicitly requests modification of the certificate using the procedures described in Section 4.7 of this CPS.

4.7.6 Publication of the modified certificate by CyberCert

4.7.6.1 Certificates will be published at the registers described in Clause 2.1 of this CPS once issued, following the conduct described in Section 4.7.5. This will be done within 1 business day.

4.7.7 Notification of certificate issuance by CyberCert to other entities

4.7.7.1 By registering the recertified and newly certified Subscriber into the publicly-accessible registry, CyberCert implicitly notifies all *CSCAU SMB1001 — Multi-tiered cyber security certification for small and medium-sized businesses* Relying Parties when a certificate is published.

5. Facility, Management, and Operational Controls

5.1 Physical controls

5.1.1 Site location and construction

5.1.1.1 CyberCert uses cloud service providers with up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC 2® certifications.

5.1.2 Physical access

5.1.2.1 CyberCert uses cloud service providers with up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC 2® certifications.

5.1.3 Power and air conditioning

5.1.3.1 CyberCert uses cloud service providers with up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC 2® certifications.

5.1.4 Water exposures

5.1.4.1 CyberCert uses cloud service providers with up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC 2® certifications.

5.1.5 Fire prevention and protection

5.1.5.1 CyberCert uses cloud service providers with up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC 2® certifications.

5.1.6 Media storage

5.1.6.1 CyberCert uses cloud service providers with up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC 2® certifications.

5.1.7 Waste disposal

5.1.7.1 CyberCert uses cloud service providers with up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC 2® certifications.

5.1.8 Off-site backup

5.1.8.1 CyberCert uses cloud service providers with up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC 2® certifications.

5.2 Procedural controls

5.2.1 Trusted roles

5.2.1.1 The following trusted roles are defined for CyberCert:

5.2.1.2 **System Administrator** – A privileged computer system user with the ability to configure or modify components of a computer system beyond the abilities of a standard user.

5.2.1.3 **Audit System Administrator** – A System Administrator for computer systems involved with audit functions, including audit trails of the System Administrators of

other production systems. Audit System Administrators have no duties on, and no access to, other production systems. Other production System Administrators have no duties on, and no access to, computer systems involved with audit functions.

5.2.1.4 **Authorising Officer (AO)** – The role of one or more (named) people in a Conformity Assessment Body (CAB) who are responsible for approving the issuing of certificates.

5.2.1.5 **Certifying Officer (CO)** – The role of one or more (named) people in a Conformity Assessment Body (CAB) who are responsible for issuing certificates.

5.2.1.6 **Certification Manager (CM)** – The role of a single (named) person in each Conformity Assessment Body (CAB) who is responsible for overseeing the management and operation of all certification components of their CAB.

5.2.1.7 **Certification Registrar (CR)** – The role of one or more (named) people in a Conformity Assessment Body (CAB) who oversee the currency and accuracy of the Registry, and are responsible for a combination of some or all of AO, CO, and CM roles.

5.2.2 Number of persons required per task

5.2.2.1 At a minimum, the Certification Registrar SHALL oversee the currency and accuracy of the Registry, and are responsible for a combination of some or all of AO, CO, and CM roles.

5.2.2.2 For Level 1, 2, and 3 certifications, the roles of CM, AO and CO may be performed by a single combined role of a Certification Registrar (CR).

5.2.2.3 Level 4 and 5 certifications require separation of duties between the AO and CO roles and, as such, the roles of the AO and CO must be performed by two separate individuals.

5.2.2.4 In all cases, the roles of the CM and the AO may be performed by the same person.

5.2.3 Identification and authentication for each role

5.2.3.1 All access is controlled via individual login with multi-factor authentication over secure connections and role-based access control (RBAC).

5.2.4 Roles requiring separation of duties

5.2.4.1 Level 4 and 5 certifications require separation of duties between the AO and CO roles and, as such, for Level 4 and Level 5 certifications, the roles of the AO and CO must be performed by two separate individuals.

5.2.4.2 Computer System Administrators and other privileged users of CyberCert's local certificate registry have all activity logged with immediate duplication to a central audit log controlled by separate Audit System Administrators.

5.2.4.3 Computer System Administrators and other privileged users of CyberCert's local certificate registry have no duties on, and no access to, computer systems involved with audit functions. Audit System Administrators have no duties on, and no access to, CyberCert's local certificate registry.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

5.3.1.1 Only CyberCert staff or approved third party contractors may fulfill the trusted roles described in Clause 5.2.1 of this CPS.

5.3.1.2 Personnel appointed to trusted roles shall:

- Maintain the highest integrity and be trustworthy;
- Have demonstrated the ability to perform their duties;
- Have no other duties that would interfere or conflict with their certification duties; and
- Be appointed by an appropriate authority, in accordance with the *CyberCert Certification Policy*.

5.3.2 Background check procedures

5.3.2.1 All CyberCert staff undergo normal employment reference checks. Appropriate vetting is used to ensure appropriate personnel security for the CM, AOs, COs, System Administrators and Audit personnel.

5.3.3 Training requirements

5.3.3.1 CyberCert provides its staff with training upon assignment to a role as well as continuing professional development training as required.

5.3.4 Retraining frequency and requirements

5.3.4.1 CyberCert provides regular refresher training and updates for all personnel as required.

5.3.5 Job rotation frequency and sequence

5.3.5.1 There are no requirements for enforced job rotation among staff fulfilling trusted roles.

5.3.6 Sanctions for unauthorized actions

5.3.6.1 Compliance with the *CyberCert Certification Policy* is a mandatory requirement. All employees must comply with the requirements of this CPS. If CyberCert staff have performed activities inconsistent with CyberCert policies and procedures, appropriate disciplinary actions are taken, in accordance with the *CyberCert Certification Policy*.

5.3.7 Independent contractor requirements

5.3.7.1 Independent contractors and consultants are contractually bound to the same conditions policies and procedures, in accordance with the *CyberCert Certification Policy*.

5.3.8 Documentation supplied to personnel

5.3.8.1 All staff or third party contractors assigned to a trusted role are provided with the *CyberCert Certification Policy* and this CPS as part of their annual training requirements.

5.4 Audit logging procedures

5.4.1 Types of events recorded

5.4.1.1 The following items will be logged and archived:

- Certificate requests,
- Conformity assessments and recommendations,
- Certificate issuance,
- Attempted and successful accesses to the systems,
- Attempted and successful changes to system configurations,
- Stopping and starting of audit and logging sub-systems, and
- Reboots of systems.

5.4.1.2 Audit records include the date, time, responsible user or process, and relevant event data.

5.4.2 Frequency of processing log

5.4.2.1 Audit logs are continually processed for significant security and operational events by automated specialist cloud audit applications with current ISO/IEC 27001 certifications.

5.4.3 Retention period for audit log

5.4.3.1 Audit logs are retained indefinitely with the most recent 90 days immediately on-hand and all older logs available within 24 hours.

5.4.4 Protection of audit log

5.4.4.1 The CyberCert local certificate registry generates immutable audit trails of register activity.

5.4.5 Audit log backup procedures

5.4.5.1 Audit logs are retained indefinitely with multiple copies around the world.

5.4.6 Audit collection system

5.4.6.1 The audit collection system is integral with CyberCert's cloud service providers who have up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC 2 certifications.

5.4.7 Notification to event-causing subject

5.4.7.1 All personnel are notified that all systems events are logged. No notification of individual events is provided to the event-causing subject.

5.4.8 Vulnerability assessments

5.4.8.1 CyberCert uses cloud service providers with up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC type 2 certifications.

5.5 Records archival

5.5.1 Types of records archived

5.5.1.1 The following records will be archived:

- Certificate requests,
- Conformity assessments and recommendations, and
- Certificate issuance.

5.5.2 Retention period for archive

5.5.2.1 Records are retained indefinitely with the most recent 24 months immediately on-hand and all older records available within 24 hours.

5.5.3 Protection of archive

5.5.3.1 Record archives are held in version control, where every change creates a new version and deleted records are marked deleted but never actually deleted.

5.5.4 Archive backup procedures

5.5.4.1 Record archives are retained indefinitely with multiple copies.

5.5.5 Timestamping of records

5.5.5.1 All data is recorded and timestamped with globally synchronised time sources.

5.5.6 Archive collection system

5.5.6.1 The archiving process moving records from short-term storage to long-term deep archive is automated and integral with CyberCert's cloud service providers who have up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC 2 certifications.

5.5.7 Procedures to obtain and verify archive information

5.5.7.1 The recovery process to obtain and verify records from long-term deep archive back into short-term storage is automated and integral with CyberCert's cloud service providers who have up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC 2 certifications.

5.6 Compromise and disaster recovery

5.6.1 The recovery process to obtain the redundant encrypted copies of records from appropriate data centres is automated and integral with CyberCert's cloud service providers who have up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC type 2 certifications.

6. Technical security controls

6.1 Certificate generation and issuing

6.1.1 Requests for certification MAY only be made by a person identified as an executive officer, owner, senior executive OR nominee of the Subscriber. See Clause 3.2.6 of this CPS.

6.1.2 Attestations on the Subscriber's compliance SHALL only be made by a person identified as an executive officer, owner OR senior executive of the Subscriber.

6.1.3 CyberCert assesses the validity of the Subscriber's attestation.

6.1.4 CyberCert either approves, rejects, or holds their decision on issuing a CyberCert certificate to the Subscriber.

6.2 Certificate protection and storage

6.2.1 CyberCert uses cloud service providers with up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC 2 certifications.

6.2.2 Read access to CyberCert's local certificate registry is public.

6.2.3 Write access to CyberCert's local certificate registry is restricted to CyberCert CRs, Cos and/or CMs.

6.3 Other aspects of certificate management

6.3.1 Requests for certificate recertifications MAY only be made by a person identified as an executive officer, owner, senior executive OR nominee of the Subscriber. See Clause 3.2.6 of this CPS.

6.3.2 Only individuals who have the appropriate authorisation, per earlier registration of account details, MAY request modification of a certificate.

6.3.3 A Subscriber MAY request certificate modification for changing the Subject name to match a new registered name as listed in the ABR, for the same ABN and/or ACN.

6.3.4 A change of ABN and/or ACN SHALL be processed as a new certification in accordance with Clause 4.1 of this CPS, in its entirety.

6.3.5 A change of certification level, other than due a CyberCert error, SHALL be processed as a recertification in accordance with Clause 4.6 of this CPS.

6.4 Attestation data

6.4.1 The following records will be archived:

- Certificate requests,
- Conformity assessments and recommendations, and
- Certificate issuance.

6.4.2 Record archives are held in version control, where every change creates a new version and deleted records are marked deleted but never actually deleted.

6.5 Computer security controls

6.5.1 CyberCert uses cloud service providers with up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC 2 certifications.

6.6 Life cycle technical controls

6.6.1 Record archives are retained indefinitely with multiple copies and with the most recent 24 months immediately on-hand and all older records available within 24 hours.

6.7 Network security controls

6.7.1 CyberCert uses cloud service providers with up-to-date ISO/IEC 27001, PCI DSS and AICPA SOC 2 certifications.

6.8 Time-stamping

6.8.1 All data is recorded and timestamped with globally synchronised time sources.

7. Certificate Profiles

7.1 CyberCert issues SMB1001 certificates for a number of different levels of attestation.

7.2 Certification is available in any one of five levels of validation and attestation, from Level 1 (minimum requirements of the standard and minimal independent validation) to Level 5 (all requirements of the standard and all independently validated).

7.3 CyberCert SMB1001 certificates consist of:

7.3.1 CyberCert identifiers and logos;

7.3.2 The Subject is identified by their registered name as listed in the Australian Business Register (ABR);

7.3.3 The Subject's ABN and/or ACN;

7.3.4 The current version of the standard being used, viz. "*CSCAU SMB1001 — Multi-tiered cyber security certification for SMBs*";

7.3.5 The Certification Level for which the Subscriber is attesting;

7.3.6 A Schedule of Conformity/Non-Conformity;

7.3.7 A QR Code to allow access to the public registry for verification;

7.3.8 The CyberCert Authorising Officer approving the certification;

7.3.9 The date of certification; and

7.3.10 The expiry date.

8. Compliance Audit and Other Assessments

8.1 Frequency or circumstances of assessment

8.1.1 CyberCert employs an independent third party to perform quarterly vulnerability assessments for all external-facing computer systems and network ports.

8.1.2 CyberCert employs an independent third party to perform annual penetration testing for all computer systems and networks.

8.2 Identity/qualifications of assessor

8.2.1 The independent third-party assessors are commercial entities specializing in IT security assessment.

8.3 Assessor's relationship to assessed entity

8.3.1 The independent third-party assessors will be organizationally independent of CyberCert and shall not have any current or planned financial, legal, or other relationship that could result in a conflict of interest during the period of the audit.

8.4 Topics covered by assessment

8.4.1 Quarterly external vulnerability scans cover all external-facing computer systems and all external-facing network ports.

8.4.2 Annual penetration testing includes all external and internal network penetration testing and all external-facing and internal-facing application penetration testing for all computer systems and networks.

8.5 Actions taken as a result of deficiency

8.5.1 CyberCert reviews all recommendations made by the external assessor and takes remedial actions as appropriate.

8.6 Communication of results

8.6.1 The independent security assessment reports are provided to the CyberCert CR or CM, and to the CyberCert Board.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or recertification fees

9.1.1.1 Certification and recertification fees are charged by CyberCert. Fees are set from time to time by CyberCert and may be reviewed.

9.1.1.2 The current schedule of fees is published on the CyberCert web site (https://cybercert.com.au/) and from within the platform (https://cybercert.au).

9.1.2 Fees for other services

9.1.2.1 CyberCert does not charge for any other services unless specified in the CPS.

9.1.3 Refund policy

9.1.3.1 CyberCert will issue a new certificate free of charge if, through the fault of CyberCert, an incorrect certificate was issued.

9.1.3.2 No refunds are provided if a fee is charged for a certificate once that certificate is issued.

9.2 Financial responsibility

9.2.1 Any party participating in the *CSCAU SMB1001 — Multi-tiered cyber security certification for small and medium-sized businesses* framework, including any Subscriber or Relying Party, is responsible for taking out and maintaining its own insurance coverage in regard to any loss or damage that may be suffered by it under this CPS or as a result of participating in the *CSCAU SMB1001* framework.

9.3 Confidentiality of business information

9.3.1 CyberCert will maintain the confidentiality of any business information received by it in accordance with any relevant contractual undertakings and any law or regulation having the force of law.

9.4 Privacy of personal information

9.4.1 CyberCert will maintain the confidentiality of any personal information received by it in accordance with any relevant contractual undertakings and any law or regulation having the force of law, including without limitation the *Privacy Act 1988 (Cth)*.

9.5 Intellectual property rights

9.5.1 Intellectual Property Rights in CyberCert materials and in any modifications or enhancements made to CyberCert materials remain, or are from the date of creation, the property of CyberCert.

9.5.2 CyberCert Subscribers and Relying Parties must ensure that CyberCert materials are, to the extent practicable, identified as the property of CyberCert and that CyberCert materials remain at all times free of any lien, charge or other encumbrance of a third party.

9.5.3 CyberCert grants to Subscribers and Relying Parties a revocable, royalty-free, nonexclusive, non-transferable licence for the term of a Subscriber's certificate.

9.6 Representations and warranties

9.6.1 CyberCert makes no representations or warranties of any kind, whether express, implied or other than what is already stated in this CPS.

9.6.2 CyberCert warrants that

- the certificate information provided to it has been accurately recorded in the certificate, certificate register and transferred to CSCAU;
- at the time of issue, a certificate contains all of the information required by CSCAU.

9.6.3 Subscriber representations and warranties are detailed in the Subscriber Agreement.

9.6.4 Relying Parties warrant that they will verify the validity of a certificate in the manner specified in the relevant policy. This includes verify that the certificate is used within the limits specified in the relevant policy.

9.6.5 Relying Parties also warrant that they will notify CyberCert if they suspect that a certificate held by a Subscriber is invalid or use in a manner not specified in the relevant policy.

9.6.6 There are no stipulations for the representations and warranties of other parties.

9.7 Disclaimers of warranties

9.7.1 EXCEPT FOR ANY WARRANTIES EXPRESSLY GIVEN IN ACCORDANCE WITH THIS CPS. NO IMPLIED OR EXPRESS WARRANTIES ARE GIVEN BY CYBERCERT OR BY ANY OTHER ENTITY WHO MAY BE INVOLVED IN THE ISSUING OR MANAGING OF CERTIFICATES ISSUED UNDER THIS CPS AND ALL STATUTORY WARRANTIES ARE TO THE FULLEST EXTENT PERMITTED BY LAW EXPRESSLY EXCLUDED.

9.7.2 CyberCert provides software for organizations to attest that they have implemented requirements meeting a certificate. However, CyberCert gives no warranty as to their correctness. CyberCert cannot be held responsible for any misuse of a certificate by a Subscriber or any unchecked acceptance of certificates by a Relying Party.

9.7.3 Any Relying Party that accepts a certificate for any usage for which it was not issued does so at its own risk and responsibility.

9.7.4 The Subscriber Agreement includes a disclaimer consistent with the above disclaimer.

9.8 Limitations of liability

9.8.1 CyberCert disclaims to the full extent permitted by law all liabilities other than already stated in this CPS.

9.9 Indemnities

9.9.1 CyberCert to the full extent permitted by law provides no indemnities other than already stated in this CPS.

9.10 Term and termination

9.10.1 This CPS remains in force until the expiry of every CyberCert issued SMB1001 certificate.

9.11 Individual notices and communications with participants

9.11.1 All communications with participants are as already stated in this CPS.

9.12 Amendments

9.12.1 Promulgation of amendments to this CPS are as already stated in this CPS.

9.13 Dispute resolution provisions

9.13.1 See 9.14 Governing law.

9.14 Governing law

9.14.1.1 These Terms and Conditions shall be exclusively governed by the laws of Queensland, Australia. The competent court in Queensland has exclusive jurisdiction with regard to disputes arising from these Terms and Conditions.

9.15 Compliance with applicable law

9.15.1.1 If any provision contained in the Terms and Conditions is held to be invalid by a court of law, this shall not in any way affect the validity of the remaining provisions.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

9.16.1.1 The CPS, any relevant policy and the Subscriber Agreement will supersede any prior agreements or representations, written or oral, between the parties to the Subscriber Agreement.

9.16.2 Assignment

9.16.2.1 No party may assign its obligations or rights under this CPS without CyberCert's prior written approval.

9.16.3 Severability

9.16.3.1 Each provision is severable and independent of any other provision.

9.16.3.2 If any provision of this CPS becomes invalid, illegal or unenforceable, then this provision will, where reasonable and possible, be read down to the extent needed to allow the provision to be not illegal, invalid or unenforceable.

9.16.3.3 If the reading down of any provision, entire or part, is not possible, then the provision or part of it will be void and severable with no impact on the remaining provisions of the CPS.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

9.16.4.1 Failure by CyberCert to enforce a provision of this CPS shall not affect the enforceability of that provision or the CPS as a whole at any point in time.

9.16.5 Force Majeure

9.16.5.1 CyberCert is not liable for any loss or damage arising from any delay or failure to perform its obligations described in this CPS if such delay is due to Force Majeure.

9.17 Other provisions

9.17.1 No other provisions are stipulated.

10. References

Chokhani, S., Ford, W., Sabett, R., Merrill, C., Wu, S.: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. RFC 3647 (2003)