

Certification Practice Statement

Version 1.1 · 10 July 2026

Copyright protected document

© CyberCert Pty Ltd 2026. This document is protected by copyright. Unauthorized reproduction, distribution or use of its content is prohibited and may have legal consequences.

The CyberCert name, logo and badges are trademarks of CyberCert Pty Ltd. Patents pending: 2023903514, 2023903509, 2023903507, 2023903506.

Email: support@cybercert.ai · Web: cybercert.ai

Document control

Preparation

Authorized by	Ryan Ettridge
Document owner	CyberCert Certification Registrar
Authors	Dr David Ross, Dr Ryan Ko, Peter Maynard (v1.1 amendments: Hester Imhof Koch, Ryan Ettridge)
Issue date	10 July 2026
Next review date	July 2027 (reviewed at least annually)
Source file	https://cybercert.ai/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
1.1	10/07/2026	All	Adopt DSI accreditation model; internationalize; remove inconsistencies; simplify wording	Hester Imhof Koch, Ryan Ettridge

Table of contents

01 Introduction

- 1.1 Overview
- 1.2 Document control
- 1.3 SMB1001 certification participants
- 1.4 Certificate usage
- 1.5 Policy administration
- 1.6 Definitions
- 1.7 Initialisms and acronyms

03 Identification and Authentication

- 3.1 Naming
- 3.2 Initial identity validation
- 3.3 Identification and authentication for recertification
- 3.4 Identification and authentication for modification

05 Facility, Management and Operational Controls

- 5.1 Physical and environmental controls
- 5.2 Procedural controls
- 5.3 Personnel controls
- 5.4 Audit logging
- 5.5 Records archival
- 5.6 Compromise and disaster recovery

07 Certificate Profiles

09 Other Business and Legal Matters

- 9.1 Fees
- 9.2 Financial responsibility
- 9.3 Confidentiality and privacy
- 9.4 Intellectual property
- 9.5 Representations and warranties
- 9.6 Disclaimers and limitations
- 9.7 Term and termination
- 9.8 Notices and amendments
- 9.9 Governing law and dispute resolution
- 9.10 Miscellaneous

02 Publication and Registry Responsibilities

- 2.1 The register
- 2.2 Publication
- 2.3 Access controls

04 Certificate Life-Cycle Operational Requirements

- 4.1 Application
- 4.2 Application processing
- 4.3 Issuance
- 4.4 Acceptance and publication
- 4.5 Certificate usage
- 4.6 Recertification
- 4.7 Modification

06 Technical Security Controls

- 6.1 Certificate generation and issuance
- 6.2 Certificate protection and storage
- 6.3 Other certificate management
- 6.4 Attestation data
- 6.5 Computer, network and life-cycle controls

08 Information Security and Independent Assessment

10 References

01 Introduction

This is a public document. It may be used by any party that relies on (a Relying Party) a certificate issued by CyberCert against the Dynamic Standards International Limited (DSI) standard SMB1001 — Multi-tiered cyber security certification standard for small and medium-sized businesses (SMB1001).

This Certification Practice Statement (CPS) describes the practices CyberCert uses, and the responsibilities of the parties involved, when issuing, recertifying and managing SMB1001 certificates. It supports the CyberCert Certification Policy, an internal document that Relying Parties do not need. This CPS contains everything a Relying Party needs to understand CyberCert's certification activities against SMB1001.

1.1 Overview

- 1.1.1 DSI is a standards development body that facilitates industry-led cyber security certification standards for small and medium-sized businesses worldwide.
- 1.1.2 CyberCert is a global Dynamic Standards Certifier (DSC), accredited by DSI to assess conformance against SMB1001 at Levels 1 to 5.
- 1.1.3 SMB1001 is a DSI multi-level cyber security certification standard for small and medium-sized businesses. It is reviewed and updated annually to keep its controls fit for the current threat environment. This CPS applies specifically to SMB1001; for certificates issued against other standards, refer to the CPS for that standard.
- 1.1.4 Certification is available at any one of five levels, from Level 1 (minimum requirements and minimal independent validation) to Level 5 (all requirements, all assertions independently validated).
- 1.1.5 For any given level, CyberCert performs only the practices listed in this CPS for that level. Relying Parties should review those practices before relying on a certificate, and must not assume that any practice not listed for a level has been performed.
- 1.1.6 This CPS describes: participants; how certificates are issued, recertified and managed; security (personnel, audit and operational controls); audit procedures; and business and legal matters.

1.2 Document control

1.2.1 Name and identification

- 1.2.1.1 This document is the CyberCert SMB1001 Certification Practice Statement (CPS). The current version is available from CyberCert, and the document history (following the cover page) lets Relying Parties assess changes relevant to existing certificates.

1.2.2 Scope

- 1.2.2.1 This CPS covers all CyberCert certification operations and activities against SMB1001 — including all assessment and validation — across every business unit and site, whether on-premises, online or via external parties, and including staff working remotely.

1.2.3 Application

- 1.2.3.1 Through the CyberCert Certification Policy, this CPS binds: all CyberCert staff (regardless of role, including agency workers, trainees and volunteers); all clients seeking or recertifying a CyberCert certification; and any Relying Party that chooses to rely on a CyberCert certification.
- 1.2.3.2 Relying Parties must not infer that any practice not listed in this CPS for a particular level has been performed by CyberCert.

1.3 SMB1001 certification participants

1.3.1 Summary

1.3.1.1 The participants are: an independent standards development body; an accreditation body; one or more Dynamic Standards Certifiers (DSCs) that assess and issue certificates; the certificate Subscribers; and the Relying Parties. Figure 1 provides an overview.

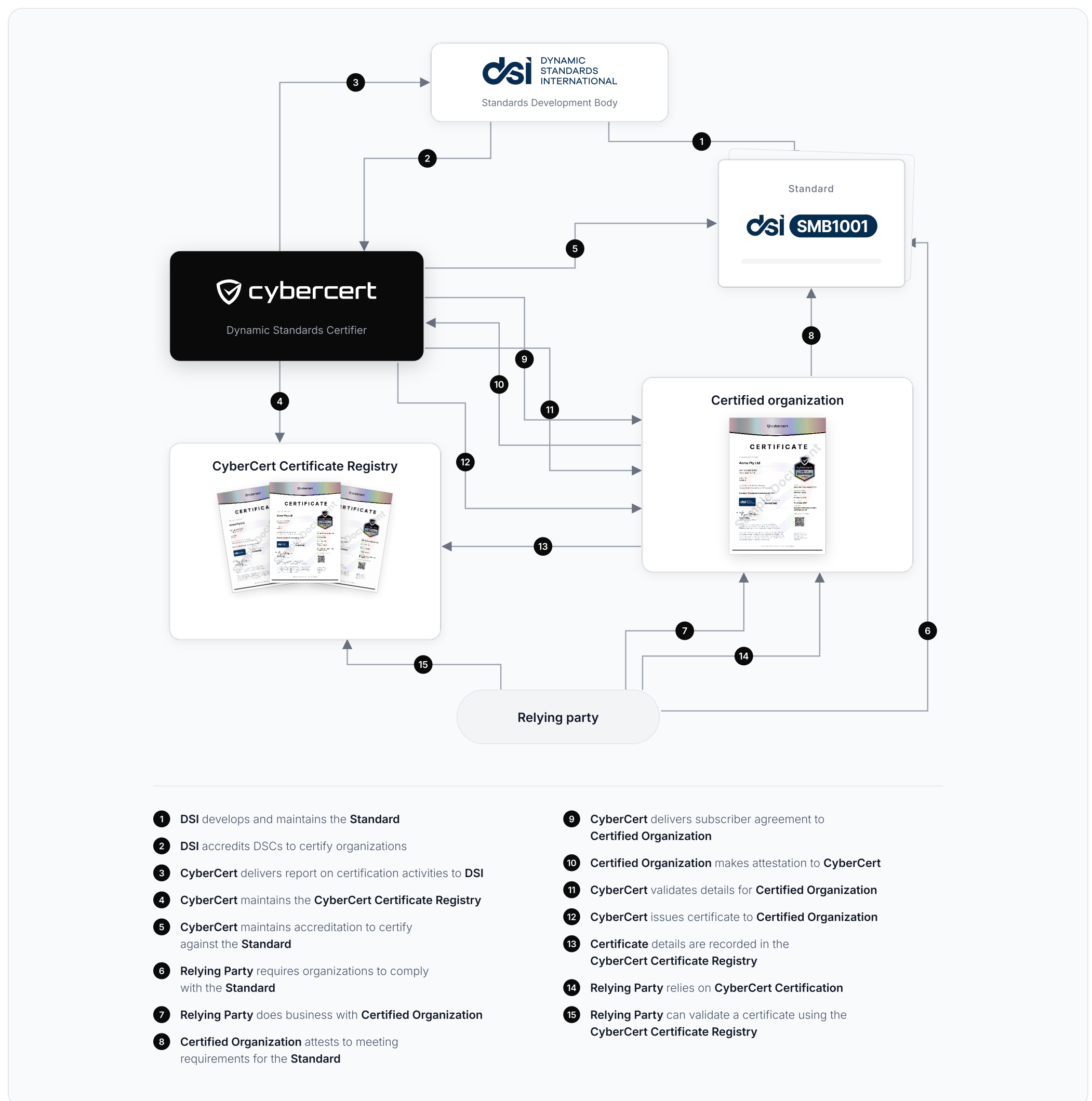


Figure 1 — The SMB1001 certification ecosystem

1.3.2 Standards development body

1.3.2.1 DSI is an independent standards development body. It comprises an executive body that manages the development of standards through a Steering Committee, and a separate, independent, skills-based Standards and Certification Oversight Board (SCOB) of subject-matter authorities that reviews and assures the quality of the executive body's outputs.

1.3.3 Accreditation body

- 1.3.3.1 The accreditation body accredits DSCs to assess Subscribers' conformance to SMB1001. Until an approved accreditation scheme for SMB1001 exists, the accreditation body is the standards development body, DSI.
- 1.3.3.2 Once an approved accreditation scheme for SMB1001 has been developed, the accreditation body will be a recognized accreditation body or a relevant Mutual Recognition Arrangement (MRA).

1.3.4 Dynamic Standards Certifiers (DSCs)

- 1.3.4.1 DSCs are the entities, accredited by the accreditation body, that assess Subscribers' conformance to SMB1001 and then generate and issue SMB1001 certificates. CyberCert is a DSC accredited by DSI.
- 1.3.4.2 Each DSC has: a single Certification Manager (CM) responsible for overseeing all certification components; one or more Authorizing Officers (AO) responsible for approving issuance; one or more Certifying Officers (CO) responsible for issuing certificates; and one or more internal or external Auditors responsible for audit and compliance.
- 1.3.4.3 For Levels 1–3, the CM, AO and CO roles may be combined into a single Certification Registrar (CR) role. For Levels 4 and 5, the AO and CO roles must be performed by two separate individuals. In all cases, the CM and AO roles may be performed by the same person.
- 1.3.4.4 CyberCert operates a register that holds issued certificates.

1.3.5 Subscribers

- 1.3.5.1 Subscribers are the organizations that apply for, or are named in, a certificate issued by a DSC. Certificates are issued to organizations, not to individuals.
- 1.3.5.2 Before a certificate is issued, every Subscriber must formally agree to the CyberCert Terms, which include acknowledgement and acceptance of all provisions of Clause 9 of this CPS. The CyberCert Terms may be accepted online. DSCs must enforce their use.

1.3.6 Relying Parties

- 1.3.6.1 Relying Parties are the entities or individuals that act in reliance on certificates issued under SMB1001. They may or may not also be Subscribers.
- 1.3.6.2 A Relying Party relies on a certificate to its stated level of certification assurance, and should satisfy itself, with due diligence, that the level asserted is suitable for its application.
- 1.3.6.3 No party is obliged to rely on any certificate. A Relying Party that chooses to rely on an SMB1001 certificate must, in doing so, agree to be bound by the obligations in this CPS.

1.3.7 Other participants

- 1.3.7.1 From time to time, external third-party auditors may be engaged to verify compliance with SMB1001.

1.4 Certificate usage

1.4.1 Appropriate uses

- 1.4.1.1 Certificates validate a particular level of attestation of a Subscriber's conformance to SMB1001.
- 1.4.1.2 In accordance with the CyberCert Terms and Clause 9, Subscribers may present, and may publicly advertise, their certificates to Relying Parties as validation of their attested level of conformance. Other uses consistent with these goals are also permitted.

1.4.2 Prohibited uses

- 1.4.2.1 Any use other than those described in Clause 1.4.1 is prohibited.

1.5 Policy administration

- 1.5.1

This CPS is administered by CyberCert. The point of contact is the CyberCert Certification Registrar, reachable via the Help contact on the CyberCert website at <https://cybercert.ai>.
- 1.5.2

CyberCert may amend this CPS from time to time. When it does, the new version is posted to the CyberCert website and the CPS URL (<https://cybercert.ai/SMB1001-CPS.pdf>) is updated to point to it.

1.6 Definitions

Audit System Administrator	A System Administrator for computer systems involved in audit functions, including audit trails of other System Administrators. Audit System Administrators have no duties on, and no access to, other production systems; and other System Administrators have no duties on, and no access to, audit systems.
Authentication	The process of verifying the claimed identity of an entity.
Authorizing Officer (AO)	The role of one or more named people in a DSC responsible for approving the issuing of certificates.
Business Register	The official register maintained by the relevant national, state or other authority that records registered business entities in a jurisdiction.
Business Registration Number (BRN)	The official identifier issued to a business entity by the relevant Business Register in its jurisdiction of registration.
Certification Manager (CM)	The role of a single named person in each DSC responsible for overseeing the management and operation of all certification components of that DSC.
Certification Practice Statement (CPS)	A document that specifies the practices a DSC employs in issuing certificates.
Certification Registrar (CR)	The role of one or more named people in a DSC who oversee the currency and accuracy of the Registry and may perform some or all of the AO, CO and CM roles.
Certifying Officer (CO)	The role of one or more named people in a DSC responsible for issuing certificates.
CyberCert Terms	The agreement between CyberCert (as DSC) and a Subscriber that establishes the rights and responsibilities of the parties regarding the issuance and management of certificates. (Also referred to as the Subscriber Agreement.)
Dynamic Standards Certifier (DSC)	An accredited authority that assesses conformance and manages SMB1001 certificates.
Evidence of Identity (EOI)	The process of determining the identity of an entity using identification documents or other identifying information, categorized as Primary and Secondary Identification Documents.
Force Majeure	Any occurrence or omission beyond a party's reasonable control that prevents or delays it from performing its obligations under this CPS, a policy or the CyberCert Terms.
Identification	The process of establishing the identity of an entity. Identification does not necessarily include authentication; most certification circumstances require both.
Identification Document	A Primary Identification Document or a Secondary Identification Document.
Participant	An individual or organization acting as a Subscriber, Relying Party, DSC, register service provider or similar entity.
Personal Information (PI)	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, as defined by applicable privacy and data protection law.
Primary Identification Document	A government-issued identification document that, on its own, reliably establishes a person's identity in a given name — for example a passport, national identity document, birth certificate or citizenship certificate.

Register	The online storage area where the DSC stores issued certificates.
Relying Party	A recipient of a certificate who acts in reliance on it.
Secondary Identification Document	An identification document, other than a Primary Identification Document, that helps establish a person's identity in a given name — for example a driver license or a government-issued benefits or entitlement card.
SMB1001 Level [1–5] certificate	A certificate issued by a DSC attesting to a named subject's conformance with the requirements of a particular level, from Level 1 to Level 5, as described in SMB1001 and this CPS.
Subscriber	An organization that is the subject of, and to whom, a certificate is issued.
System Administrator	A privileged user able to configure or modify components of a computer system beyond the abilities of a standard user.
Validation	The process of identifying and verifying conformity details.

1.7 Initialisms and acronyms

AO	Authorizing Officer	BRN	Business Registration Number
CM	Certification Manager	CO	Certifying Officer
CPS	Certification Practice Statement	CR	Certification Registrar
DSC	Dynamic Standards Certifier	DSI	Dynamic Standards International Limited
EOI	Evidence of Identity	MRA	Mutual Recognition Arrangement
PI	Personal Information	SCOB	Standards and Certification Oversight Board
UTC	Coordinated Universal Time		

02 Publication and Registry Responsibilities

2.1 The register

- 2.1.1 CyberCert maintains an authoritative, publicly searchable register of all certificates it issues, and the register generates immutable audit trails of register activity.
- 2.1.2 For each certificate, the register records:
- Subscriber organization name;
 - certificate ID;
 - date the certificate was issued;
 - name of the Subscriber officer, and the attesting officer;
 - contact email and/or phone number for that officer;
 - certification status and the level completed; and
 - version/release of the standard attested to.

2.2 Publication

- 2.2.1 CyberCert publishes issued certificates to its certificate registry, accessible at <https://verify.cybercert.ai>, within one working day of issuance, and shares the registry with DSI as required by this CPS or any relevant policy.

2.3 Access controls

- 2.3.1 Read access to the certificate registry is public. Write access is restricted to CyberCert COs and the CyberCert CM; AOs do not have write access.
- 2.3.2 For Level 4 and Level 5 certification, a CO cannot issue a certificate without a successful audit by an AO, and an AO cannot issue certificates. This separation of duties is enforced procedurally.
- 2.3.3 All activity by System Administrators and other privileged users of the registry is logged, with immediate duplication to a central audit log controlled by separate Audit System Administrators. Privileged registry users have no access to audit systems, and Audit System Administrators have no access to the registry.

03 Identification and Authentication

3.1 Naming

- 3.1.1 The subject of each certificate is identified by its registered legal name and Business Registration Number (BRN) as listed in the relevant Business Register. The subject name appears exactly as listed there; there is no provision to add trading or other names.
- 3.1.2 Certificates are not issued anonymously or pseudonymously. Subject names are unique within the scope of the relevant Business Register.
- 3.1.3 Where a name in the Business Register includes trademarks or service marks, they appear as part of the registered name but are not identified as such.
- 3.1.4 Where a Subscriber's jurisdiction does not maintain a public business register or issue a business registration number, CyberCert identifies the subject using the business's registered legal name and any equivalent official company identification number available in that jurisdiction (see Clause 3.2.4).

3.2 Initial identity validation

3.2.1 Setting the organization name

- 3.2.1.1 Subscribers supply their BRN at initial registration. CyberCert validates it in the relevant Business Register, records the registered entity name, and uses only that name in all business documents, the CyberCert Terms and any certificate issued.
- 3.2.1.2 Where a Subscriber's jurisdiction does not maintain a public business register or issue a business registration number, the Subscriber must contact CyberCert and provide the information in Clause 3.2.4.

3.2.2 Authentication of organization identity

- 3.2.2.1 CyberCert obtains approved Subscriber BRNs from its clients and partners. An organization cannot initiate certification until its BRN has been supplied by a CyberCert client or partner, and CyberCert validates that BRN in the relevant Business Register.

3.2.3 Authentication of individual identity

- 3.2.3.1 CyberCert may have existing business relationships with its clients and partners. New clients must establish a business relationship with CyberCert before transacting.
- 3.2.3.2 Individual officers of Subscribers are not authenticated in order to request certification or recertification, but must be authenticated to request a modification or a revocation.
- 3.2.3.3 To authenticate an individual, a CyberCert AO, CO or CM sights — in person or via live video link — at least one Primary Identification Document, or at least two Secondary Identification Documents.
- 3.2.3.4 The validating officer records that authentication occurred but does not record the authentication data itself. Specifically, they record their own name and role, the name of the individual identified, the nature of the EOI sighted (for example, passport with issuing country, or driver license with issuing jurisdiction) and the date. They do not record the actual document, or any number, code or other detail from it.
- 3.2.3.5 No Personal Information is collected or stored except the individual's name, role and any contact information relevant to the certification process.

3.2.4 Where no business register applies

- 3.2.4.1 A Subscriber whose jurisdiction does not maintain a public business register or issue a business registration number must provide CyberCert with:
- full company name;
 - country of incorporation or registration;
 - the name of the foreign body that registered the business;
 - company identification number;
 - registered business address;
 - business type (private, publicly listed, majority-owned subsidiary of a publicly listed company, or a regulated entity in its home jurisdiction); and
 - directors.

- 3.2.4.2 CyberCert verifies this information by searching the relevant foreign registration bodies. 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 information

- 3.2.5.1 No non-verified Subscriber information 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 officer, owner or senior executive of the Subscriber, identified and authenticated in accordance with Clause 3.2.3.
- 3.2.6.2 Subscribers must notify CyberCert when a previously authorized officer is no longer authorized to act on their behalf.

3.2.7 Interoperation

- 3.2.7.1 CyberCert SMB1001 certifications are fully compatible with SMB1001 certifications issued by any other DSC accredited by DSI.

3.3 Identification and authentication for recertification

- 3.3.1 A Subscriber's current (not expired) CyberCert certification is sufficient for both identification and authentication for recertification. CyberCert re-validates the BRN in the relevant Business Register and records any change to the registered entity name.
- 3.3.2 Existing validated officers are not re-validated as individuals, but their roles as executive officer, owner or senior executive are re-validated. New or additional officers are validated under Clause 3.2.3. Subscribers must notify CyberCert when an authorized officer is no longer authorized.
- 3.3.3 An expired certification is not sufficient for identification or authentication; recertification of an expired certification, or of a non-CyberCert certification, is processed as a new certification under Clause 3.2 in its entirety.

3.4 Identification and authentication for modification

- 3.4.1 A Subscriber's current (not expired) CyberCert certification is sufficient for both identification and authentication to: correct a CyberCert error (not a change) in a certificate's subject name, level or relevant date; or change the subject name to match a new registered name in the Business Register for the same BRN.
- 3.4.2 For a change of certification level, a current certification is sufficient for identification, and for authentication at the same or a lower level. It is not necessarily sufficient for authentication at a higher level; for a higher level, the identification and authentication rules for recertification at that level apply.
- 3.4.3 A change of BRN is processed as a new certification under Clause 3.2 in its entirety. Any change of dates is processed as a recertification under Clause 3.3.

- 3.4.4 An expired certification is not valid; no historic corrections are considered, and any change to an expired certification is processed as a new certification under Clause 3.2 in its entirety.

04 Certificate Life-Cycle Operational Requirements

4.1 Application

- 4.1.1 A certification request may only be made by a person identified as an officer, owner, senior executive or nominee of the Subscriber (see Clause 3.2.6).
- 4.1.2 The enrolment process is:
- an officer requests a CyberCert account for a particular BRN;
 - the account holder registers at <https://cybercert.ai/> and is linked to that account;
 - the account holder answers a series of questions for an initial assessment of conformance to the SMB1001 requirements;
 - the system offers an appropriate level of attestation; and
 - the Subscriber's representative requests to proceed, providing their attestation for the requested level.

4.2 Application processing

- 4.2.1 At registration, the system validates the BRN and displays the registered name from the relevant Business Register. The Subscriber must accept the name shown or supply a different BRN, then create or provide their CyberCert account credentials.
- 4.2.2 CyberCert assesses the attestation and approves, rejects or holds the application, communicating the outcome to the Subscriber through its system.
- 4.2.3 CyberCert expects to issue a certificate within a reasonable time after approval, generally within one business day.
- 4.2.4 A Subscriber has twelve (12) months from the date of purchase of the subscription (as set out in the CyberCert Terms) to complete a certification. If it is not completed within that period, the subscription expires.

4.3 Issuance

- 4.3.1 Certificate issuance is handled by CyberCert's internal systems. The Subscriber is notified of issuance through the CyberCert platform at <https://certification.cybercert.ai/> and by email to the address provided during attestation.

4.4 Acceptance and publication

- 4.4.1 A Subscriber is deemed to have accepted a certificate unless it explicitly requests modification under Clause 4.7.
- 4.4.2 Once accepted, certificates are published to the register described in Clause 2.1 within one business day. By registering a certified Subscriber in the public registry, CyberCert implicitly notifies all SMB1001 Relying Parties.

4.5 Certificate usage

- 4.5.1 Certificates validate a particular level of attestation of a Subscriber's conformance to SMB1001. In accordance with the CyberCert Terms and Clause 9, Subscribers may present, and publicly advertise, their valid certificates to Relying Parties as validation of their attested level. Other consistent uses are permitted. Expired certificates must not be used.
- 4.5.2 A Relying Party may rely on a valid certificate to its stated level of assurance, and should satisfy itself, with due diligence, that the level is suitable for its application. It is the Relying Party's responsibility to verify that a certificate is not expired.

4.6 Recertification

- 4.6.1 CyberCert notifies the Subscriber at least three (3) months before the expiry date. Issued certificates are not renewable; recertification produces a new certificate.
- 4.6.2 A recertification request 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), via <https://cybercert.ai/>. Recertification of a non-CyberCert certification is processed as a new certification under Clauses 4.1–4.3.
- 4.6.3 The outcome is communicated to the Subscriber, and the Subscriber is notified of issuance of the new certificate through the platform and by email. Acceptance, publication and Relying-Party notification follow Clauses 4.4.1 and 4.4.2.

4.7 Modification

- 4.7.1 A Subscriber may request modification to correct a CyberCert error (not a change) in a certificate's subject name, level or relevant date, or to change the subject name to match a new registered name for the same BRN. A change of BRN is processed as a new certification under Clause 4.1; a change of level (other than to correct a CyberCert error) under Clauses 4.1–4.3; and any change of dates as a recertification under Clause 4.6.
- 4.7.2 Either the Subscriber or CyberCert may initiate a modification, but only individuals with the appropriate authorisation (per their registered account details) may request one. Requests are made via the Help system on the platform at <https://cybercert.ai>.
- 4.7.3 The Subscriber is notified of issuance of a modified certificate by the platform. Acceptance, publication and Relying-Party notification follow Clauses 4.4.1 and 4.4.2.

5.1 Physical and environmental controls

- 5.1.1 CyberCert's certification operations are hosted by cloud service providers holding current ISO/IEC 27001, PCI DSS and AICPA SOC 2 certifications; there is no CyberCert-controlled physical site for these purposes. All physical and environmental controls — site security and construction, physical access, power, air conditioning, water exposure, fire prevention and protection, media storage, waste disposal and off-site backup — are provided by those cloud service providers under those certifications.

5.2 Procedural controls

- 5.2.1 The trusted roles at CyberCert are System Administrator, Audit System Administrator, Authorizing Officer (AO), Certifying Officer (CO), Certification Manager (CM) and Certification Registrar (CR), as defined in Clause 1.6.
- 5.2.2 At a minimum, the CR oversees the currency and accuracy of the Registry and may perform some or all of the AO, CO and CM roles. For Levels 1–3, these roles may be combined in the CR. For Levels 4 and 5, the AO and CO roles must be performed by two separate individuals. In all cases, the CM and AO roles may be performed by the same person.
- 5.2.3 All access is controlled via individual login with multi-factor authentication over secure connections, using role-based access control (RBAC).
- 5.2.4 All activity by System Administrators and other privileged users of the registry is logged, with immediate duplication to a central audit log controlled by separate Audit System Administrators. Privileged registry users have no access to audit systems, and Audit System Administrators have no access to the registry.

5.3 Personnel controls

- 5.3.1 Only CyberCert staff or approved third-party contractors may fill the trusted roles in Clause 5.2.1.
- 5.3.2 Personnel appointed to trusted roles must:
- 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 under the CyberCert Certification Policy.
- 5.3.3 All staff undergo standard employment reference checks, with appropriate vetting for the CM, AOs, COs, System Administrators and audit personnel.
- 5.3.4 CyberCert provides training on assignment to a role, plus regular refresher training and continuing professional development as required. There is no enforced job rotation among trusted roles.
- 5.3.5 Independent contractors and consultants are contractually bound to the same policies and procedures under the CyberCert Certification Policy. All staff and contractors in trusted roles receive the CyberCert Certification Policy and this CPS as part of their annual training.
- 5.3.6 Compliance with the CyberCert Certification Policy is mandatory. Where staff act inconsistently with CyberCert's policies and procedures, appropriate disciplinary action is taken under that Policy.

5.4 Audit logging

- 5.4.1 The following are logged and archived: certificate requests; conformity assessments and recommendations; certificate issuance; attempted and successful system access; attempted and successful configuration changes; stopping and starting of audit and logging sub-systems; and system reboots. Each record includes the date, time, responsible user or process, and relevant event data.
- 5.4.2 Logs are processed continuously for significant security and operational events by automated specialist cloud audit applications under current ISO/IEC 27001 certification.
- 5.4.3 Audit logs are retained indefinitely, with the most recent 90 days immediately on hand and older logs available within 24 hours, backed up with multiple copies worldwide. The registry generates immutable audit trails.
- 5.4.4 All personnel are notified that all system events are logged; no notification is given for individual events. Vulnerability assessments of the underlying infrastructure are covered by the cloud service providers' certifications referenced in Clause 5.1. CyberCert also operates its own vulnerability and penetration testing program over its platform and applications.

5.5 Records archival

- 5.5.1 Certificate requests, conformity assessments and recommendations, and certificate issuance records are archived. Records are retained indefinitely, with the most recent 24 months immediately on hand and older records available within 24 hours.
- 5.5.2 Archives are held under version control: every change creates a new version, and deleted records are marked deleted but never actually removed. All data is timestamped against globally synchronized time sources.
- 5.5.3 Archiving and recovery between short-term storage and long-term deep archive are automated and integral to CyberCert's cloud service providers, which hold current ISO/IEC 27001, PCI DSS and AICPA SOC 2 certifications.

5.6 Compromise and disaster recovery

- 5.6.1 Recovery of redundant encrypted copies of records from appropriate data centres is automated and integral to CyberCert's cloud service providers, which hold current ISO/IEC 27001, PCI DSS and AICPA SOC 2 certifications. Security incidents, including any suspected compromise or data breach, are managed and reported under CyberCert's documented incident-response procedures.

06 Technical Security Controls

6.1 Certificate generation and issuance

- 6.1.1 A certification request 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). Attestations of the Subscriber's compliance may only be made by an executive officer, owner or senior executive.
- 6.1.2 CyberCert assesses the validity of the attestation and then approves, rejects or holds its decision on issuing a certificate.

6.2 Certificate protection and storage

- 6.2.1 Certificate storage relies on cloud service providers holding current ISO/IEC 27001, PCI DSS and AICPA SOC 2 certifications. Read access to the registry is public; write access is restricted to CyberCert CRs, COs and/or CMs. Certificate and registry data is encrypted in transit and at rest, and all platform access follows least-privilege principles.

6.3 Other certificate management

- 6.3.1 Recertification requests 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). Only individuals with the appropriate authorisation (per their registered account details) may request a modification.
- 6.3.2 A Subscriber may request modification to change the subject name to match a new registered name for the same BRN. A change of BRN is processed as a new certification under Clause 4.1; a change of level (other than to correct a CyberCert error) as a recertification under Clause 4.6.

6.4 Attestation data

- 6.4.1 The attestation data archived is as set out in Clause 5.5. Archives are held under version control: every change creates a new version, and deleted records are marked deleted but never actually removed.

6.5 Computer, network and life-cycle controls

- 6.5.1 Computer security and network security controls are provided by cloud service providers holding current ISO/IEC 27001, PCI DSS and AICPA SOC 2 certifications. Record archives are retained indefinitely with multiple copies, the most recent 24 months immediately on hand and older records available within 24 hours. All data is timestamped against globally synchronized time sources.

07 Certificate Profiles

7.1 CyberCert issues SMB1001 certificates at all five levels, from Level 1 (minimum requirements and minimal independent validation) to Level 5 (all requirements, all independently validated).

7.2 Each CyberCert SMB1001 certificate contains:

- CyberCert identifiers and logos;
- the subject's registered name as listed in the relevant Business Register;
- the subject's Business Registration Number (BRN) and any additional local company identification number;
- the current version of the standard ("DSI SMB1001 — Multi-tiered cyber security certification for SMBs");
- the certification level attested to;
- a schedule of conformity/non-conformity;
- a QR code linking to the public registry for verification;
- the CyberCert Authorizing Officer approving the certification;
- the date of certification; and
- the expiry date.



Sample SMB1001 Level 5 certificate

08 Information Security and Independent Assessment

- 8.1 CyberCert maintains an Information Security Policy that is updated regularly to meet the maximum practical cyber security requirements needed to protect the information and systems used in its certification activities, in accordance with its obligations under this CPS.
- 8.2 CyberCert engages independent third parties to assess the security of its systems. Those assessors are commercial entities specializing in IT security assessment, are organizationally independent of CyberCert, and have no current or planned financial, legal or other relationship that could create a conflict of interest during the assessment period.
- 8.3 CyberCert reviews all recommendations from independent assessors and takes remedial action as appropriate. Assessment reports are provided to the CyberCert CR or CM and to the CyberCert Board.

9.1 Fees

- 9.1.1 CyberCert charges certification and recertification fees, set and reviewed by CyberCert from time to time. The current fee schedule is published on the CyberCert website (<https://cybercert.ai>) and within the platform.
- 9.1.2 CyberCert may charge for other services related to the fulfilment of its duties as a DSC.
- 9.1.3 If CyberCert issues an incorrect certificate through its own fault, it issues a corrected certificate free of charge. Otherwise, no refund is provided once a certificate has been issued.

9.2 Financial responsibility

- 9.2.1 Every party participating in the SMB1001 framework, including any Subscriber or Relying Party, is responsible for taking out and maintaining its own insurance for any loss or damage it may suffer under this CPS or as a result of participating in the DSI SMB1001 framework.

9.3 Confidentiality and privacy

- 9.3.1 CyberCert maintains the confidentiality of business information and Personal Information it receives, in accordance with its contractual undertakings and applicable privacy and data protection laws.

9.4 Intellectual property

- 9.4.1 Intellectual property rights in CyberCert materials, and in any modifications or enhancements to them, remain (or from creation become) the property of CyberCert.
- 9.4.2 Subscribers and Relying Parties must, so far as practicable, ensure CyberCert materials are identified as CyberCert's property and kept free of any third-party lien, charge or other encumbrance.
- 9.4.3 CyberCert grants Subscribers and Relying Parties a revocable, royalty-free, non-exclusive, non-transferable license for the term of a Subscriber's certificate.

9.5 Representations and warranties

- 9.5.1 CyberCert makes no representations or warranties of any kind, whether express, implied or otherwise, beyond those stated in this CPS.
- 9.5.2 CyberCert warrants that certificate information provided to it has been accurately recorded in the certificate and register and transferred to DSI; and that, at the time of issue, a certificate contains all information required by DSI.
- 9.5.3 Subscriber representations and warranties are set out in the CyberCert Terms.
- 9.5.4 Relying Parties warrant that they will verify the validity of a certificate as specified in the relevant policy, that it is used within the limits specified, and that they will notify CyberCert if they suspect a certificate is invalid or is being used other than as specified. No representations or warranties are stipulated for other parties.

9.6 Disclaimers and limitations

- 9.6.1 Except for warranties expressly given under this CPS, no implied or express warranties are given by CyberCert or by any other entity involved in issuing or managing certificates under this CPS, and all statutory warranties are excluded to the fullest extent permitted by law.
- 9.6.2 CyberCert provides software for organizations to attest that they have implemented the requirements for a certificate, but gives no warranty as to the correctness of those attestations. CyberCert is not responsible for any misuse of a certificate by a Subscriber or any unchecked acceptance of a certificate by a Relying Party.
- 9.6.3 A Relying Party that accepts a certificate for a use for which it was not issued does so at its own risk. The CyberCert Terms include a disclaimer consistent with this clause.
- 9.6.4 To the fullest extent permitted by law, CyberCert disclaims all liabilities, and provides no indemnities, beyond those stated in this CPS.

9.7 Term and termination

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

9.8 Notices and amendments

- 9.8.1 Communications with participants, and the promulgation of amendments to this CPS, are as stated elsewhere in this CPS.

9.9 Governing law and dispute resolution

- 9.9.1 This CPS and the CyberCert Terms are governed by, and disputes are subject to the exclusive jurisdiction specified in, the CyberCert Terms. If any provision is held invalid by a court, the remaining provisions are unaffected.

9.10 Miscellaneous

- 9.10.1 Entire agreement. This CPS, any relevant policy and the CyberCert Terms supersede any prior agreements or representations, written or oral, between the parties to the CyberCert Terms.
- 9.10.2 Assignment. No party may assign its obligations or rights under this CPS without CyberCert's prior written approval.
- 9.10.3 Severability. Each provision is severable and independent. If a provision becomes invalid, illegal or unenforceable, it will, where reasonable and possible, be read down to the minimum extent needed to make it valid; if that is not possible, it is void and severable, with no effect on the remaining provisions.
- 9.10.4 Enforcement. CyberCert's failure to enforce a provision does not affect the enforceability of that provision or of this CPS as a whole at any time.
- 9.10.5 Force Majeure. CyberCert is not liable for any loss or damage arising from delay or failure to perform its obligations under this CPS where that delay or failure is due to Force Majeure.

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).