Certification Practice Statement (CPS)

Version: 1.0

Date: 23/09/2024

Contents

1 Introduction

This Certification Practice Statement (CPS) of the "SoftStarter Root Certification Authority" (hereinafter, "SoftStarter CA") applies to the services of the SoftStarter CA that are associated with the issuance of and management of digital certificates. This CPS can be found on the AuCom softstart hub at www.cyber.softstarterhub.com. This CPS may be updated from time to time.

This CPS addresses the technical, procedural, and personnel policies and practices of the CA in all services and during the complete life cycle of certificates as issued by the SoftStarter CA. The SoftStarter CA is operated and owned by AuCom Electronics Limited. Inquiries on this SoftStarter CA CPS can be addressed to: cyber@aucom.com.

This CPS is final and binding between AuCom Electronics Ltd. (operating and owning the SoftStarter CA), a company under public law, with a registered office at 123 Wrights Road, Addington, Christchurch 8024, New Zealand, (Hereinafter referred to as "AuCom") and the Subscriber and/or Relying Parties, who use, rely, or attempt to rely upon certification services made available by the SoftStarter CA.

This SoftStarter CA will be used for digital signing of firmware code and therefore Subscribers to this CPS are 1) AuCom Electronics Ltd. and 2) Benshaw Applied Motor Controls, who are both members of the Benshaw Group. Relying Parties are those entities who purchase and use cybersecure products that have been manufactured by the Subscribers, and who rely upon the digital signature to ensure that the embedded firmware is genuine and has not been altered or modified in any way.

1.1 Overview

This CPS applies to the specific domain of the SoftStarter CA. The purpose of this CPS is to present the AuCom practices and procedures in managing certificates and to demonstrate best practice pertaining to the issuance and security of digital certificates. The certificate type addressed in this CPS is the following:

- Firmware signing certificates

These certificates can be used **only** to authenticate AuCom embedded firmware and executable modules.

This CPS identifies the roles, responsibilities, and practices of all parties involved in the life cycle, use, reliance upon, and management of AuCom certificates. The provisions of this CPS with regard to practices, level of services, responsibilities, and liability bind all parties involved including the SoftStarter CA, Subscribers, and Relying Parties.

This document is the Certification Practice Statement applicable to the signing PKI used to sign firmware and software used in AuCom products.

1.2 Document Name and Identification

AuCom ensures compliance of its certificates with the requirements and assertions of this CPS.

1.3 PKI Participants

The SoftStarter CA makes its services available to AuCom certificate Subscribers. These Subscribers include without limitation entities that uses the AuCom certificates for the purposes of:

- Authentication (digital signature)
- Encryption

1.3.1 SoftStarter Certification Authority

A Certification Authority, such as SoftStarter CA, is an organization that issues digital certificates to be used in this context for code signing. A certification authority is also referred to as the Issuing Authority to denote the purpose of issuing certificates.

The SoftStarter CA drafts and implements the policy prevailing in issuing a certain type or class of digital certificates.

The SoftStarter CA ensures the availability of all services pertaining to the management of AuCom certificates, including without limitation the issuing, revocation, status verification of a certificate, as they may become available or required in specific applications.

Appropriate publication is necessary to ensure that Relying Parties obtain notice or knowledge of functions associated with the revoked and/or suspended certificates. Publication is manifested by including a revoked or suspended certificate in a Certificate Revocation List (CRL) that is published in an online directory / repository.

The domain of responsibility of the SoftStarter CA comprises the overall management of the certificate lifecycle including the following actions:

- Issuance
- Revocation
- Renewal
- Status validation

1.3.1.1 Role of SoftStarter CA

SoftStarter CA operates as a Trust Service Provider to deliver Trust Services to a user community.

1.3.2 Relying Parties

Relying Parties are natural or legal persons that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in SoftStarter CA's certificate. The Relying Party can use the certificate to verify the integrity of signed code. Relying Parties are solely responsible for deciding whether to rely on the information from the SoftStarter CA and agree that they have enough information to make an informed decision.

To verify the validity of a digital certificate, Relying Parties must always refer to SoftStarter CA revocation information such as a Certificate Revocation List published on AuCom's specified directory / repository. Certificate validation takes place prior to relying on information featured in a certificate. Relying Parties meet specific obligations as described in this CPS.

1.4 Certificate Usage

Certain limitations apply to the use of SoftStarter CA certificates.

1.4.1 Appropriate Certificate Usage

SoftStarter CA certificates will be used to validate the authenticity and integrity of signed firmware.

Additional uses are specifically designated once they become available to end entities.

1.4.2 Prohibited Certificate Usage

End entity certificate use is restricted by using certificate extensions on key usage and extended key usage. Any usage of the certificate inconsistent with these extensions is not authorized.

1.4.3 Certificate Extensions

SoftStarter CA issues certificates that might contain extensions defined by the X.509 v3 standard as well as any other applicable formats.

1.4.4 Critical Extensions

SoftStarter CA uses certain critical extensions in the certificates it issues such as:

- A basic constraint in the certificate to show whether a certificate is meant for a CA or not.
- To show the intended usage of the key.

1.5 Policy Administration

The Policy Managing Authority of the SoftStarter CA manages this AuCom CPS. The SoftStarter CA registers, observes the maintenance, and interprets this CPS. The SoftStarter CA makes available the operational conditions prevailing in the life-cycle management of AuCom certificates.

1.5.1 Scope

AuCom may make revisions and updates to its policies as it sees fit or as required by the circumstances. Such updates become binding for all certificates that have been issued or are to be issued 30 days after the date of the publication of the updated version of the CPS.

1.5.2 AuCom Policy Management Authority

New versions and publicized updates of AuCom policies are approved by the AuCom Policy Management Authority. The AuCom Policy Management Authority in its present organizational structure comprises of members as indicated below:

- At least one member of the management of SoftStarter CA.
- At least one authorized agent directly involved in the drafting and development of AuCom practices and policies.

1.5.3 Acceptance of Updated Version of the CPS

Upon approval of a CPS update by the AuCom Policy Management Authority, that CPS is published in the AuCom online Repository at www.cyber.softstarterhub.com

The updated version is binding against all existing and future Subscribers unless notice is received within 30 days after communication of the notice. After such period the updated version of the CPS is binding against all parties including the Subscribers and parties relying on certificates that have been issued under a previous version of the AuCom CPS.

SoftStarter CA publishes on its web site at least the two latest versions of its CPS.

1.5.4 Version Management and Denoting Changes

Changes are denoted through new version numbers for the CPS. New versions are indicated with an integer number followed by one decimal that is zero. Minor changes are indicated through one decimal number that is larger than zero. Minor changes include:

- Minor editorial corrections.
- Changes to contact details.

1.6 Definitions and Acronyms

A list of definitions can be found at the end of this CPS.

2 Publication and Repository Responsibilities

SoftStarter CA publishes information about the digital certificates that it issues in an online repository. SoftStarter CA reserves its right to publish certificate status information on third party repositories.

SoftStarter CA retains an online repository of documents where it makes certain disclosures about its practices, procedures and the content of certain policies including this CPS. SoftStarter CA reserves its right to make available and publish information on its policies by any appropriate means within the AuCom repository.

All parties who are associated with the issuance, use or management of AuCom certificates are hereby notified that SoftStarter CA may publish submitted information on publicly accessible directories in association with the provision of electronic certificate status information.

SoftStarter CA refrains from making publicly available certain elements of documents including security controls, procedures, internal security polices etc.

3 Identification and Authentication (I&A)

SoftStarter CA maintains appropriate procedures to address naming practices, including the recognition of trademark rights in certain names.

SoftStarter CA authenticates the requests of parties wishing to revoke certificates under this policy.

3.1 Initial Identity Validation

Not Applicable.

3.2 I&A for Re-Key requests

Not Applicable.

3.3 I&A for Revocation Requests

For the identification and authentication procedures of revocation requests, SoftStarter CA requires using an a request addressed to the SoftStarter CA at cyber@aucom.com

4 Certificate Life-Cycle Operational Requirements

The following operational requirements apply to Certificate Lifecycle.

All entities within the AuCom domain including Subscribers or other participants have a continuous duty to inform the SoftStarter CA of all changes in the information featured in a certificate during the operational period of such certificate and until it expires or is revoked.

To carry out its tasks AuCom may use third party agents for which SoftStarter CA assumes responsibility.

4.1 Certificate Application Processing and Issuance

A Subscriber requests digital signing certificate applications from SoftStarter CA. The SoftStarter CA validates the submitted information. Subsequently, the application is either approved or rejected.

Following issuance of the approved certificate, the SoftStarter CA delivers the issued certificate to the Subscriber.

4.2 Certificate Generation

With reference to the issuance and renewal of certificates, SoftStarter CA represents towards all parties that certificates are issued securely according to the conditions set below:

- The procedure to issue a certificate is securely linked to the associated registration, including the provision of any Subscriber generated public key.
- The confidentiality and integrity of registration data is ensured at all times through appropriate SSL (Secure Socket layer) links.
- Certificate requests and generation are also supported by robust and tested procedures that have been scrutinized for compliance with the prevailing standards.

4.3 Certificate Acceptance

An issued AuCom certificate is deemed accepted by the Subscriber when no objection is received by AuCom from the Subscriber within three (3) working days after it being received. Any objection to accepting an issued certificate must explicitly be notified to the SoftStarter CA. The reasoning for rejection including any fields in the certificate that contain erroneous information must also be submitted.

The SoftStarter CA might post the issued certificate on a repository. The SoftStarter CA also reserves its right to notify the certificate issuance by the SoftStarter CA to other entities.

4.4 Key Pair and Certificate Usage

The responsibilities relating to the use of keys and certificates include the ones addressed below:

4.4.1 Relying Party

The obligations of the Relying Party include the following ones:

4.4.1.1 Relying Party Duties

A party relying on a AuCom certificate will:

- Validate a AuCom certificate by using certificate status information (e.g. CRL) published by SoftStarter CA.
- Trust a SoftStarter CA certificate only if all information featured on such a certificate can be verified via such a validation procedure as being correct and up to date.
- Rely on a AuCom certificate, only as it may be reasonable under the circumstances.
- Trust a certificate only if it has not been revoked.

4.5 Certificate Renewal

No stipulation. All certificate issuance, including re-issuing certificates intended for the same devices but with different keys, lifetimes, or other fields, is subject to the same requirements described in this document.

4.6 Certificate Revocation

The SoftStarter CA revokes a AuCom certificate if:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key of the certificate's subject.
- The certificate's Subscriber or Relying Party has breached a material obligation under this CPS.
- The performance of a person's obligations under this CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, another person's information is materially threatened or compromised.
- There has been a modification of the information contained in the certificate of the certificate's subject.

4.7 Certificate Status Services

Certificate Revocation Lists (CRLs) will only be used for publishing certificate status. Firmware signing certificates will be unable to be verified by offline hardware.

4.8 Key Escrow and Recovery

A second HSM is used as a backup for key pairs in case the primary HSM is stolen, damaged or corrupted.

5 Management, Operational and Physical Controls

This section describes non-technical security controls used by SoftStarter CA to perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival. All entities performing CA functions implement and enforce the following physical, procedural, logical, and personnel security controls for a CA.

5.1 Physical Security Controls

The SoftStarter CA implements physical controls on its own, leased, or rented premises.

The SoftStarter CA infrastructure is logically separated from any other certificate management infrastructure, used for other purposes.

The SoftStarter CA secure premises are located in an area appropriate for high-security operations.

Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones.

The SoftStarter CA implements prevention and protection as well as measures against fire exposures.

Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.

The sites of the SoftStarter CA host the infrastructure to provide the SoftStarter CA services. The SoftStarter CA sites implement proper security controls, including access control, intrusion detection and monitoring. Access to the sites is limited to authorized personnel listed on an access list.

5.1.1 PKI Equipment

The PKI equipment consists of a computer and a physical FIPS 140-3 Level 3 Hardware Security Module (HSM). The computer and HSM are both used offline (i.e. air-gapped and not connected to any network) so as to provide a high level of security to hacking and malware. The computer is used for digital signing and is not used for any other purpose.

The HSM contains all private keys and these are never transmitted out of the HSM except in an encrypted form for safety backup to another HSM. A second HSM is used as a backup in case the primary HSM is stolen, damaged or corrupted. Certificates are stored on the computer as a reference.

5.1.2 PKI Equipment Storage

When the PKI equipment is not being used, it is stored in a secure safe that is keycode protected and is fire and water resistant, and data protection rated. The second backup HSM is stored in a similar secure safe in a different location.

5.1.3 Password Management

Passwords for access to the SoftStarter CA are stored in handwritten form in physical log books associated with the PKI hardware.

5.2 Procedural Controls

The SoftStarter CA follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of the electronic signature-related technologies.

The SoftStarter CA obtains a signed statement from each member of the staff on not having conflicting interests, maintaining confidentiality, and protecting personal data.

All members of the staff operating the key management operations such as developers, administrators, security officers, and system auditors or any other roles that materially affect such operations are considered as serving in a trusted position.

The SoftStarter CA conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make a reasonable attempt to determine their trustworthiness and competence.

Where dual control is required, at least two trusted members of the SoftStarter CA staff need to bring their respective and split knowledge in order to be able to proceed with an ongoing operation.

The SoftStarter CA ensures that all actions with respect to the SoftStarter CA can be attributed to the system and the person of the CA that has performed the action.

The SoftStarter CA implements dual control for critical CA functions.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, Clearances

The SoftStarter CA performs checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job.

5.3.2 Training Requirements and Procedures

The SoftStarter CA makes available training for their personnel to carry out their functions.

5.3.3 Retraining Period and Retraining Procedures

Periodic training updates might also be performed to establish continuity and updates in the knowledge of the personnel and procedures.

5.3.4 Sanctions Against Personnel

SoftStarter CA sanctions personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems for the purpose of imposing accountability on a participant's personnel, as it might be appropriate under the circumstances.

5.3.5 Controls of Independent Contractors

Independent contractors and their personnel are subject to the same privacy protection and confidentiality conditions as SoftStarter CA personnel.

5.3.6 Documentation for Initial Training and Retraining

The SoftStarter CA make available documentation to personnel, during initial training, retraining, or otherwise.

5.4 Audit Logging Procedures

Audit logging procedures include event logging and audit systems, implemented for the purpose of maintaining a secure environment. SoftStarter CA implements the following controls:

SoftStarter CA audit records events that include but are not limited to:

- Access to the PKI equipment
- Issuance of a certificate.
- Revocation of a certificate.
- Publishing of a CRL.

Audit trail records contain:

- The identification of the operation.
- The date and time of the operation.
- The identification of the certificate, involved in the operation.
- The identification of the person that performed the operation.

Documents available include:

- Configuration of hardware and software.
- Personnel access lists.

SoftStarter CA ensures that designated personnel review log files at regular intervals and detect and report anomalous events.

Log files and audit trails are archived for inspection by the authorized personnel of SoftStarter CA.

5.5 Records Archival

SoftStarter CA keeps archives in a retrievable format.

SoftStarter CA ensures the integrity of the physical storage media and implements proper copying mechanisms to prevent data loss.

Archives are accessible to authorized personnel of SoftStarter CA as appropriate. The SoftStarter CA keeps internal records of the following items:

- All certificates for a period of a minimum of 2 years after the expiration of the certificate.
- Audit trails on the issuance of certificates for a period of a minimum of 2 years after issuance of a certificate.
- Audit trail of the revocation of a certificate for a period of a minimum of 2 years following the revocation of a certificate.
- CRLs for a minimum of 1 years after expiration or revocation of a certificate.
- Support documents on the issuance of certificates for a period of 2 years after expiration of a certificate. Support documents can be electronically stored.

5.5.1 Types of Records

SoftStarter CA retains in a trustworthy manner records of SoftStarter CA digital certificates, audit data and log files.

5.5.2 Retention Period

SoftStarter CA retains in a trustworthy manner records of certificates for at least 2 years.

5.5.3 Protection of Archive

SofStarter CA stores Log records and archives in a fireproof, flood-proof safe .

5.5.4 Archive Collection

The SoftStarter CA archive collection system is internal.

5.5.5 Procedures to Obtain and Verify Archive Information

To obtain and verify archive information SoftStarter CA maintains records under clear hierarchical control.

The SoftStarter CA retains records in electronic or in paper-based format. The SoftStarter CA may require Subscribers, or their agents to submit documents appropriately in support of this requirement.

5.6 Compromise and Disaster Recovery

In a separate internal document, the SoftStarter CA documents applicable incident, compromise, reporting, and handling procedures. The SoftStarter CA documents the recovery procedures used if computing resources, software, and/or data are corrupted or suspected of being corrupted.

The SoftStarter CA establishes the necessary measures to ensure full recovery of the service, in an appropriate time frame depending on the type of disruption, in case of a disaster, corrupted servers, software or data.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 CA Key Pair Generation

Key pair generation will be performed using FIPS 140-3 Level 3 validated cryptographic modules and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys.

CA key pair generation shall create a verifiable audit trail documenting that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used.

6.1.2 Private Key Protection and Cryptographic Module Engineering Controls.

Private keys are protected by being stored in FIPS 140-3 Level 3 validated cryptographic Hardware Security Modules (HSMs). These do not allow the private keys to leave the modules, except in an encrypted form for the purpose of backing up to another HSM. A primary module is used for signing and the private keys are backed up to another module for disaster recovery.

7 Certificate and CRL profiles

This section specifies the certificate format and CRL formats.

7.1 Certificate Profile

SoftStarter CA certificate profiles are available upon request.

7.2 CRL Profile

This will be made available at the discretion of the SoftStarter CA, on request from parties explaining their interest.

8 Compliance Audit and Other Assessment

SoftStarter CA accepts under condition the auditing of practices and procedures it does not publicly disclose. SoftStarter CA gives further consideration and evaluates the results of such audits before possibly implementing them.

Following its own approval with regard to the scope and content, SoftStarter CA accepts compliance audits to ensure it meets requirements, standards, procedures, and service levels according to this CPS and accreditation schemes it publicly claims compliance with.

9 Other Business and Legal Matters

Certain legal conditions apply to the issuance of the AuCom certificates under this CPS as described in this section.

9.1 Fees

Not Applicable.

9.2 Provision

The SoftStarter CA makes this service available on an “as is” basis.

9.3 Confidentiality of Business Information

SoftStarter CA observes data privacy rules and confidentiality rules as described in the AuCom CPS. Confidential information includes:

- Any personal identifiable information, other than that contained in a certificate.
- Reason for the revocation of a certificate, other than that contained in published certificate status information.
- Audit trails.
- Correspondence regarding CA services.
- CA Private key(s).

The following items are not confidential information:

- Certificate and their content.
- Status of a certificate.

SoftStarter CA does not release nor is it required to release any confidential information without an authenticated and justified request specifying either:

- The party to whom the SoftStarter CA owes a duty to keep information confidential is the party requesting such information.
- A court order.

Parties requesting and receiving confidential information are granted permission on the assumption that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties.

9.3.1 Disclosure Conditions

Non-confidential information can be disclosed to any Subscriber and Relying Party under the conditions below:

- Only a single certificate is delivered per inquiry by Subscriber or Relying Party.
- The status of a single certificate is provided per inquiry by a Subscriber or Relying Party.

Confidential information may not be disclosed to Subscribers nor Relying Parties. SoftStarter CA properly manages the disclosure of information to the CA personnel.

To incorporate information by reference, SoftStarter CA might use computer-based and text- based pointers that include URLs, etc.

9.4 Privacy of Personal Information

Not Applicable.

9.5 Intellectual Property Rights

SoftStarter CA owns and reserves all intellectual property rights associated with its databases, web sites, certificates and any other publication whatsoever originating from SoftStarter CA including this CPS.

The Distinguished Names in use across SoftStarter CA, remain the sole property of SoftStarter CA, which enforces these rights.

Certificates are and remain property of SoftStarter CA. SoftStarter CA permits the reproduction and distribution of certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full, except that certificates are not published in any publicly accessible repository or directory without the express written permission of SoftStarter CA. The scope of this restriction is also intended to protect Subscribers against the unauthorized re-publication of their personal data featured on a certificate.

SoftStarter CA owns and reserves all intellectual property rights associated with its own products and services that it has not explicitly transferred or released to another party.

9.6 Representations and Warranties

SoftStarter CA uses this CPS to convey legal conditions of usage of AuCom certificates to Subscribers and Relying Parties.

Participants that may make representations and warranties include SoftStarter CA, Subscribers, Relying Parties, and any other participants as it might become necessary.

All parties of the AuCom domain, including the SoftStarter CA and Subscribers warrant the integrity of their respective private key(s). If any such party suspects that a private key has been compromised, they will immediately notify SoftStarter CA.

9.6.1 AuCom Repository Conditions

Parties (including Relying Parties) accessing the SoftStarter CA certificate repository agree with the provisions of this CPS and any other conditions of usage that AuCom may make available. Parties demonstrate acceptance of the conditions of usage of the CPS by submitting a query with regard to the status of a digital certificate or by anyway using or relying upon any such information or services provided. The SoftStarter CA repositories include or contain:

- Information provided as a result of the search for a digital certificate.
- Information to verify the status of an AuCom certificate.
- If a repository becomes aware of or suspects the compromise of a private key, it will immediately notify SoftStarter CA.

The SoftStarter CA maintains a certificate repository during the application period and for a minimum of two years after the expiration or revocation of a certificate.

9.6.2 Reliance at Own Risk

It is the sole responsibility of the parties accessing information published in SoftStarter CA repositories to assess and rely on information featured therein. Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a certificate. SoftStarter CA takes steps necessary to update its records and directories concerning the status of the certificates and issue warnings about. Failure to comply with the conditions of usage of the AuCom repositories may result in terminating the relationship between the SoftStarter CA and the party.

9.6.3 Accuracy of Information

SoftStarter CA makes every effort to ensure that parties accessing its repositories receive accurate, updated, and correct information. SoftStarter CA, however, cannot accept any liability beyond the limits set in this CPS.

9.6.4 Information Incorporated by Reference into a Digital Certificate

SoftStarter CA incorporates by reference the following information in every digital certificate it issues:

- Terms and conditions of the SoftStarter CA CPS.
- Any other applicable certificate policy as may be stated on an issued AuCom certificate.
- The mandatory elements of the standard X.509.
- Any non-mandatory but customized elements of the standard X.509.
- Content of extensions and enhanced naming that are not fully expressed within a certificate.
- Any other information that is indicated to be so in a field of a certificate.

9.6.5 Pointers to Incorporate by Reference

To incorporate information by reference AuCom uses computer-based and text-based pointers. AuCom may use URLs, OIDs etc.

9.7 Disclaimers of Warranties

This section includes disclaimers of express warranties.

9.7.1 Limitation for Other Warranties

SoftStarter CA does not warrant:

- The accuracy of any unverifiable piece of information contained in certificates.
- The accuracy, authenticity, completeness, or fitness of any information contained in, free, test or demo certificates.

9.7.2 Exclusion of Certain Elements of Damages

In no event is SoftStarter CA liable for:

- Any loss of profits.
- Any loss of data.
- Any indirect, consequential, or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures.
- Any transactions or services offered or within the framework of this CPS.
- Any other damages except for those due to reliance on the verified information in a certificate, except for information featured on, free, test or demo certificates.
- Any liability incurred in any case if the error in such verified information is the result of fraud or wilful misconduct of the applicant.

9.8 Indemnities

This section contains the applicable indemnities.

To the extent permitted by law, the Subscriber agrees to indemnify and hold SoftStarter CA and AuCom harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees that may be incurred as a result of:

- Failure to protect the Subscriber's private key.
- Use of a trustworthy system as required.
- Taking precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key.
- Attend to the integrity of the managed Branded Root.

9.9 Term and Termination

This CPS remains in force until notice of the opposite is communicated by SoftStarter CA on its repository.

Notified changes are appropriately marked by an indicated version. Following publications, changes become applicable 30 days thereafter.

9.10 Individual Notices and Communications with Participants

SoftStarter CA accepts notices related to this CPS by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from SoftStarter CA the sender of the notice deems its communication effective. The sender must receive such acknowledgment within twenty (20) business days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows. Individual's communications made to SoftStarter CA must be addressed to cyber@aucom.com or by post to the AuCom in the address mentioned in the introduction of this document.

9.11 Amendments

Changes to this CPS are indicated by appropriate numbering.

9.12 Dispute Resolution Procedures

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) parties agree to notify SoftStarter CA of the dispute with a view to seek dispute resolution.

Upon receipt of a Dispute Notice, SoftStarter CA convenes a Dispute Committee that advises AuCom management on how to proceed with the dispute. The Dispute Committee convenes within twenty (20) business days from receipt of a Dispute Notice. The Dispute Committee is composed by a counsel, a member of SoftStarter CA operational management and a security officer. The counsel or data protection officer chair the meeting. In its resolutions the Dispute Committee proposes a settlement to SoftStarter CA executive management. SoftStarter CA executive management may subsequently communicate the proposed settlement to the resting party.

9.13 Governing Law

The governance for this CPS is under the applicable laws of New Zealand.

9.14 Compliance with Applicable Law

SoftStarter CA complies with applicable laws of New Zealand.

9.15 Miscellaneous Provisions

9.15.1 Survival

The obligations and restrictions contained under section *9 Other Business and Legal Matters* survive the termination of this CPS.

9.15.2 Severability

If any provision of this CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CPS should be interpreted in such manner as to effectuate the original intention of the parties.

10 Definitions

10.1 Certification Authority (CA)

An organization that issues digital certificates to be used (in this context) for firmware signing.

10.2 Certification Practice Statement (CPS)

A statement of the practices that a Certification Authority employs in issuing and managing public key certificates.

10.3 Certificate Revocation List (CRL)

A CRL lists all revoked and suspended certificates during the application period. CRLs for the different products are pointed to from within the certificate through the CDP extension.

10.4 Distinguished Name

An identifier that uniquely represents an object in the X.500 directory information tree.

10.5 Relying Parties

Relying Parties are natural or legal persons that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in SoftStarter CA's certificate. The Relying Party can use the certificate to verify the integrity of signed code. Relying Parties are those entities who purchase and use cybersecure products that have been manufactured by the Subscribers, and who rely upon the digital signature to ensure that the embedded firmware is genuine and has not been altered or modified in any way.

10.6 Subscribers

This SoftStarter CA will be used for digital signing of firmware code and therefore Subscribers to this CPS are 1) AuCom Electronics Ltd. and 2) Benshaw Applied Motor Controls, who are both members of the Benshaw Group.