SECOM Trust.net Root1 CA
CERTIFICATE POLICY/ CERTIFICATION PRACTICE STATEMENT

May 22, 2006
Version 2.00

SECOM Trust Systems Co.,Ltd.

Revision History		
Version	Date	Description
V1.00	2003.08.01	Initial Draft (Translated from Japanese version)
V1.10	2003.09.29	Correction in Personnel Risks, 1.2 Overview of Security Policy Correction in 11.2.11 Certificate Status Information
V2.00	2006.05.22	The company name "SECOM Trust.net" is changed to " SECOM Trust Systems " along with the company integration. " SECOM Trust.net Security Policy Committee" is changed to " SECOM Trust Systems CA Service Improvement Committee".

Important Notice to ALL READERS:

This Certification Practice Statement (CPS) and enclosed Certificate Policy (CP) describe the practices and conditions for the provision for SECOM Trust.net Root1 CA. This CPS is translated into English for convenience of English speakers, and ALL READER of this CPS MUST understand that Japanese version is the original and English version is not formal one. In case there may be any difference in content between English version and Japanese version, Japanese version is formal and has priority in any conditions. Please check with Japanese version about formal contents.

INDEX

1 INTRODUCTION

SECOM Trust.net Root1 CA Certification Practice Statement (CPS) provides notice to all persons who use or rely on certificates issued by the SECOM Trust.net Root1 CA (THE CA).
SECOM Trust Systems Co.,Ltd. (SECOM Trust Systems) establishes THE CA to issue and manage digital certificates in support of Subscribers' activities such as digital signature or identity authentication.

> Note 1: SECOM Trust Systems purchased the CA key of "Valicert Class 1 Policy Validation Authority" from Valicert Inc. on July 23, 2003. SECOM Trust Systems manages the CA key safely and provides service to subscribers and relying parties according to the CPS. THE CA issues certificates including the expression "E=info@valicert.com CN=http://www.valicert.com/ OU=ValiCert Class 1 Policy Validation Authority O=ValiCert, Inc. L=ValiCert Validation Network", though the issuer body is SECOM Trust Systems after the purchase.

The CPS discloses several business related matters, including limitations on liability, disclaimers of warranty, limitations on damages, indemnifications, hold harmless provisions and dispute resolution process. These matters are disclosed in a SECOM Trust.net Root1 CA Certification Policy (CP) that forms a part of the CPS. The CPS and enclosed CP discribe the certification infrastructure of THE CA.

The subscribers and relying parties are to accept both the CPS and enclosed CP before using or relying upon the certificates issued by THE CA. When using the certificates issued by THE CA, subscribers and relying parties are responsible for accessing THE CA Repository (Note 2) to confirm that records indicate that the certificate is currently has not been revoked and to receive and check notice of any revision to the CPS.

> Note 2: THE CA Repository has information concerning the certificates issued by THE CA such as the CPS and CRL. For more detailed information, refer to the website (http://repository.secomtrust.net/rootrepository/).

Business relations between subscribers and SECOM Trust Systems are normally governed by written agreement. In the event of conflict between the CPS and a written agreement, the written agreement shall control the obligations, rights and duties of the parties.

1.1 Overview of Certification Practices

THE SECOM Trust.net Root1 CA

The services of THE CA provide its subscribers and relying parties with a level of assurance that the public key contained in a public key certificate does indeed belong to the entity named in the certificate. The digital signature placed on the public key certificate by the CA provides a cryptographic binding between the entity's name and other information in the certificate such as an expiry date for the binding.
For a relying party to determine whether the certificate was issued by the CA, the relying party must verify the CA's signature on the certificate using the CA signature verification key. The signature verification keys of THE CA is preloaded into widely available Web browser software (for example, Netscape Navigator or Microsoft Internet Explorer). This enable relying parties to authenticate THE CA signature using THE CA signature verification key to determine whether the certificate was issued by THE CA.

The goal of THE CA is to securely manage the life cycle of THE CA issued certificates, which may include the steps of issuance, rekey and revocation. THE CA performs all registration functions directly. THE CA is also responsible for communicating revocation notices though the issuance of Certificate Revocation Lists (CRLs). THE CA posts valid certificates and CRLs to THE CA Repository to record certificate status.

THE CA Subscribers

A subscriber here means a subordinate CA to which THE CA issues certificates.

Subscriber Initial Registration & Certificate Publication

Each subscriber is subject to initial registration in order to commence the certificate lifecycle. Initial registration consists of key generation followed by certificate issuing.
After initial registration, an issued certificate may be subsequently published in THE CA Repository in order to register it as valid.

- Subscriber generates his or her own public/private key pair using the subscriber's cryptographic equipment normally. The subscriber demonstrates to THE CA that he or she can use the subscriber's cryptographic equipment and the private component of the public/private key pair to make a digital signature on a certificate-signing request, without disclosing the private key. Upon receipt of the certificate signing request ("CSR"), THE CA ensures that it can verify the digital signature of the CSR using the public component of the public/private key pair that is indicated within the certificate signing request.

The actions taken to issue a certificate occur only upon completion of key generation actions, which included verification of the association between THE CA subscriber and the public key to be included in the subscriber's certificate.

- THE CA issues THE CA subscriber's certificate. THE CA digitally signs the certificate with a certificate-signing key. THE CA publishes the subscriber's certificate after the subscriber receives it. This enables relying parties to confirm the authenticity and integrity of the certificate.
- Based on the review of the contents of the issued certificate by both THE CA and THE CA subscriber, the certificate is published by THE CA. THE CA issued certificate is not valid until published. Assuming the subscriber confirms the accuracy of the certificate and otherwise accepts it, THE CA publishes the certificate in THE CA Repository. This act of publication makes the certificate officially available to other users valid. A valid certificate initially has no recorded revocation notices issued against it.
- THE CA Repository is an online, electronic certificate registration database that enables THE CA to publish certificates and certificate revocation notices that THE CA may subsequently issue against the certificate.
- THE CA Repository is maintained by THE CA. Relying parties may access the records in the repository to obtain current, unexpired certificates of other THE CA subscribers and their status information. For example, if an unexpired THE CA subscriber's certificate were revoked by THE CA, THE CA Repository would contain a revocation notice on a Certificate Revocation List ("CRL"). The CRL and the revocation notices that it communicates indicate that the subscriber's certificate has been revoked and should not be relied upon. The relying parties should not rely upon an expired certificate and should not rely upon a revoked certificate.
- THE CA posts certificates and CRLs to THE CA Repository in order to manage valid THE CA subscriber certificates. Subscribers and relying parties may access the records in THE CA Repository to retrieve this management information. Because THE CA certificates and CRLs are digitally signed by THE CA, they cannot be changed, maliciously or otherwise, without detection. Subscribers and relying parties should access the certificates and CRLs, detect any change and use the information to decide if they should use or rely upon a given THE CA subscriber's certificate.

Business Practices Disclosure

THE CA discloses its key and certificate life cycle management business and information privacy practices in the form of the CPS and the CP. In the form of the CPS and the CP, information regarding THE CA's business practices is available to all

subscribers and all potential relying parties from THE CA Repository.

Service Integrity

Effective key management controls and practices are essential to the trustworthiness of THE CA public key infrastructure. Cryptographic key management controls and practices cover CA key generation, CA key storage, backup and recovery, CA public key distribution, CA key usage, CA key destruction, CA key archival, the management of CA cryptographic hardware through its life cycle. Strong key life cycle management controls are vital to guard against the key compromise which can damage the integrity of THE CA public key infrastructure.

The subscriber's certificate lifecycle is the core of the services provided by THE CA. The subscriber's certificate lifecycle includes the following:

- Registration (meaning, the identification and authentication process related to binding the subscriber to the public-key in a certificate).
- The renewal of certificates.
- The rekey of certificates.
- The revocation of certificates.
- The timely publication of certificate status information through CRLs.

Environmental Controls

The establishment and maintenance of a trustworthy CA environment is essential to the reliability of THE CA's business processes. THE CA carries out proper environmental controls to manage efficiently the keys and certificates through their lifecycle.

1.2 Overview of Security Policy

SECOM Trust Systems has developed an internal security policy to ensure that corporate objectives concerning THE CA are achieved at acceptable risk.
In developing a comprehensive security policy, SECOM Trust Systems is taking positive steps to reduce risk to acceptable levels in the interests of staff, stockholders, subscribers and relying parties.

Risk

Considering the importance of the security nature of THE CA, SECOM Trust Systems do risk analysis and risk assessment, so that THE CA takes a necessary action based upon the result of the risk assessment. In the process of establishing ISMS (Information Security Management System), certified by the independent assessing agency in Japan, THE CA defines the appropriate procedure for risk assessment. The top managements

of SECOM Trust Systems understand the result of assessment and accept the risk, determine the next step to further reduce the risk. For the risk proper to THE CA, especially the risk of compromised the keys, THE CA analyze the process step by step for compromising THE CA key in order to prevent such key compromise or possibility of compromise. THE CA Personnel are well trained about the necessary operations to prevent the key compromise or its possibility.

Asset Classification and Control

A fundamental element of any security policy is the ability to classify assets and control them. If the correct tools are not available when required either a task has to be postponed, or increased risks have to be accepted. Therefore, all major assets will be clearly identified and assigned to the responsibility of the individuals in charge of THE CA. As assets are issued, they will be registered and periodic asset checks will be carried out. THE CA Personnel will be equipped to perform their duties efficiently.

Personnel Risks

THE CA has rules on an operation, which describe procedures including the controls to reduce the personnel risks, and each personnel are well trained according to them. It is the duty of each THE CA Personnel to report any problems promptly through their normal reporting mechanisms. All SECOM Trust Systems employees are to report any problems by company rules. Recovery procedure from any unusual state caused by human errors or any other problems is established. All the employees are under a pledge of confidentiality and required to understand the importance of the operation involved and to have the awareness as security professionals.

Physical and Environmental Risk

In SECOM Trust Systems all appropriate precautions physically and environmentally to operate THE CA safely is considered, including the strength of housing and equipments, the redundancy and monitoring networks and important systems.
In addition, access to entrance of the data center and each room is controlled at 7 tiers of security levels and only the authorized personnel are able to enter the room and access resources in the room. All the important equipments and systems are monitored 24 hours a day, 365 days a year. Finding an unusual event, personnel check where the problems come from and take necessary actions to recover to the usual state smoothly.

Network Management Policy

SECOM Trust Systems generally uses a centralized monitoring and audit system to cover the online information systems and network resources involved with THE CA. This support system is based on the compartmentalization of the systems and a division of duties. Over a period, the technologies employed to achieve this approach will

undoubtedly change as the information technology in general changes ever more frequently. The monitoring system will watch for anomalous behavior within the networks and report this to THE CA Personnel, and then THE CA Personnel provide instructions to operators for further detailed investigation and action. An audit system will record details of important data transactions such as operation of THE CA Private Key, so that in the event of an incident it will be possible that changes can be made effectively to counter a repeat of the incident.

Access Control

Access Control is a fundamental requirement of a reliable security policy. Effective access control means that every authorized user will be able to access resources necessary to objective achievement. To provide the effective access control system, access controls physically to the hardware and software of THE CA Computer systems and THE CA Repository is implemented and strictly restricted by the authorized personnel. Not only physical access controls but also logical access controls are introduced. Access to the hardware and software of THE CA services is recorded. The authorization of access to THE CA System is approved by THE CA's administrator explicitly

Development and Maintenance

Many resources of THE CA will potentially be subject to development and/or maintenance during their working lives. All development work will be conducted according to appropriate methodologies and be fully documented. Maintenance will be carried out as appropriate and authorized, with a maintenance log kept to record all defects, repairs, and preventative actions. The operators of equipment will be responsible for notifying any faults to the appropriate person. Only qualified personnel will perform any repair or carry out maintenance of any equipment. Where third parties are admitted to site, they will be supervised and escorted according to those rules specifically applicable to that activity. Where equipment is to be sent off site to an approved repairer or maintainer, all the necessary and appropriate precautions will be carried out as directed in respect to that particular equipment, such as information leak prevention.

Business Continuity Planning

Under the SECOM Trust Systems Security Policy, which contains a business continuity policy, the disaster recovery plan to restore the computer-related elements of THE CA is established. The main purpose of the plan is that a critical business operations to identify the problems is clearly described so that the service be provided in a reasonably timely manner following interruption to, or failure of critical processes. In complying the plan, THE CA maintains the necessary resources and means to recover the critical

component and minimize the service interruption.

Compliance

All the operation and the services of THE CA are compliant by the information security policy of SECOM Trust Systems and the CPS. Each Personnel relating to THE CA understands fully the provisions of the CPS and the information security policy. They have the training and security awareness education to understand fully the contents and intension of those provisions. The supervising personnel checks and makes sure that each work comply the provisions of the CPS and the information security policy. In order to check the compliance of the operation of THE CA the internal audit is conducted periodically.

1.3 Identification

The services of THE CA are to issue certificates to THE CA subscribers and manage the certificates through their lifecycle.

THE CA issues certificates in compliance with the CPS and the CP. The CPS encloses the CP and the current revision is published in THE CA Repository.

The subscriber's certificates are to be issued in accordance with the CP enclosed in this CPS. The CP associated in this CPS refines the practices performed by THE CA Personnel when issuing and managing the certificates.

1.4 Community and Applicability

These practices are applicable to all certificates issuing and management actions performed by THE CA personnel. They also control the use of and reliance on THE CA certificate and THE CA's Certificate Revocation List (CRL) by relying parties. All persons who use or rely upon a THE CA certificate and THE CA CRL or who use THE CA Repository are considered relying parties bound to the CPS.

THE CA issues a certificate to a subscriber in accordance with the CPS and the associated CP. This CA is a “Root” CA as it has the authority to issue a “CA-certificate” to a “subordinate” CA. The CA certificate is issued with the intention that parties relying on a certificate and/or CRL issued by the subordinate CA shall verify the digital signature on such certificate and/or CRL by using and relying upon the CA-certificate.

1.5 Contact Information

The organization administering this CPS and enclosed CP is the SECOM Trust Systems CA Service Improvement Committee. Inquiries concerning this CPS and enclosed CP will be accepted by e-mail and should be addressed as follows:

SECOM Trust Systems Co.,Ltd.
SECOM CA Support Center
e-mail address: root1-support@secomtrust.net

2. OBLIGATIONS OF THE PARTIES

2.1 THE CA Notification Obligation

Using THE CA, SECOM Trust Systems will:

- Operate THE CA according to the CPS and enclosed CP, as revised from time-to-time and as published in THE CA Repository.
- Issue and publish certificates in a timely manner.
- Revoke a certificate issued by THE CA, upon receipt of a valid request to revoke the certificate.
- Update CRLs based on issuance of a revocation notice, upon the expiry of a revoked certificate or based on the need to update an expiring CRL/
- Publish latest CRLs in THE CA Repository.
- Notify subscribers and relying parties of THE CA of certificate issuance and/or revocation by providing them with access to published and unexpired certificates and/or the latest CRLs via THE CA Repository.

2.2 THE CA Verification Obligations

THE CA directly performs all applicant registration functions. It will:

- Confirm the identity of a certificate applicant prior to publication of an issued certificate.
- Verify that a subscriber accepts a certificate prior to publishing it to the THE CA Repository.
- Validate a request to revoke a certificate.
- Reconfirm the identity of a subscriber who requests renewal or rekey of his or her valid, un-expired certificate prior to publication of the renewed or rekeyed certificate.

2.3 THE CA Repository Obligations

SECOM Trust Systems is obliged to operate THE CA Repository. To make a THE CA issued certificate valid, THE CA will publish the certificate to THE CA Repository in a timely manner.

THE CA will publish CRLs and revisions to this document in a timely manner to THE CA Repository.

THE CA subscribers and relying parties may normally directly access THE CA Repository via the Internet.

2.4 Subscriber Obligations

THE CA subscribers should:

- Provide information to THE CA that is accurate and complete to the best of the subscribers' knowledge and belief and to promptly notify THE CA of any changes to this information.
- Safeguard their private key from compromise
- Use certificates exclusively for legal purposes and in accordance with the SECOM Trust Systems CPS.
- Promptly request that THE CA revoke the subscriber's certificate if the subscriber has reason to believe there has been a compromise or suspected of a compromise of the private key corresponding to the public key listed in the certificate or a material event relating to any information listed in the certificate.

2.5 Relying Party Obligations

All the relying parties of THE CA service should:

- Rely on certificates issued by THE CA only for the purposes intended by THE CA, as stated in the CPS or any relevant CP.
- Verify the status of a certificate at the time of reliance, that the certificate is not revoked, by retrieving suitable revocation notice information from CRLs that they access at the time of reliance from THE CA Repository. Verify the status of a certificate at the time of reliance, that the certificate is not expired.
- Verify the digital signature of a certificate issued by THE CA using THE CA public key in THE CA certificate at the time of reliance the certificate issued by THE CA.
- Agree to be bound by the provisions of limitations of liability and any other restrictions, as described in the CPS, when using or relying on THE CA certificate.

3. RESPONSIBILITIES OF THE PARTIES

3.1 Limitations on use of THE CA Certificates

Certificates issued by THE CA are limited for use in connection with current SECOM Trust Systems services or particular services or products of current THE CA Customers who are in good standing with SECOM Trust Systems. Certificates issued by THE CA may not be used for any other purpose. THE CA certificates may only be used within the scope of applicable laws and regulations.

3.2 Apportionment of Liabilities between the Parties

SECOM Trust Systems total liability per certificate issued by THE CA of any form of warranties is limited to direct damages having a maximum amount of yen (meaning, a liability cap) of 1,000,000, regardless of the cause of a lawsuit, the number of transactions, digital signatures or the number of subscribers and/or relying parties relating to the certificate issued by THE CA or any association with the certificate.

In no event shall SECOM Trust Systems be obligated to pay more than the aggregate liability cap for each certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.

3.3 Limited Warranties of THE CA

3.3.1 Warranty

As THE CA, SECOM Trust Systems will issue and revoke certificates and perform other key management services and guarantee the reliability of THE CA private key in compliance with the provisions of this CPS and associated CP.

3.3.2 Limitations of Liability

SECOM Trust Systems shall not be liable for any indirect damages, special damages, incidental or secondary damages in conjunction with the warranty as stated in Section 3.3.1 Warranty. SECOM Trust Systems shall not be liable for lost earnings, lost data or other indirect or secondary damages.

3.3.3 Indemnification

SECOM Trust Systems shall not be liable for any damages under the previously stated warranty conditions in the following cases:

- Any direct or indirect damages resulting from illegal acts, improper usage or negligence not due to SECOM Trust Systems relating to the service.
- Any financial or other damages resulting from transactions involving a certificate

requested by a Subscriber or relying party.

- Any damages resulting from subscriber's software defects, bugs or other operational issues.
- Any damages due to the disclosure of individual information in a certificate or CRL.
- Any damages resulting from the improper functioning of data link and communications not due to SECOM Trust Systems.
- Any damages resulting from the unforeseen development of hardware or software for encryption algorithm deciphering technology.
- Any damages due to war, natural disasters or other acts of God causing THE CA operation stoppage.

3.4 Indemnification by Subscribers and Relying Parties

By their applying for and receiving a THE CA issued certificate, or by otherwise relying upon such certificates, subscribers, and relying parties, agree to indemnify, defend, and hold SECOM Trust Systems, its officers, directors, employees, subsidiaries, affiliates, subcontractors, consultants, suppliers, vendors, representatives, and agents harmless from any errors, omissions, acts, failures to act, or negligence resulting in liability, losses, damages, suits, or expenses of any kind, due to or otherwise proximately caused by from the subscriber's failure to provide THE CA with current, accurate, and complete information at the time of certificate application or by the relying parties errors, omissions, acts, failures to act, and negligence.

3.5 No Fiduciary Relationships

THE CA is not the agent, fiduciary, trustee, or any other representative of a THE CA subscriber or any relying party.

3.6 Governing Law

Irrespective of where THE CA, Subscriber or relying party are located, the laws of Japan shall govern the interpretation and validity of this CPS and/or associated CP and any disputes with regards to THE CA service as provided by SECOM Trust Systems. Negotiation, arbitration and the location of litigation shall be the exclusive jurisdiction of an appropriate legal institution located within the wards of Tokyo.

3.7 Changes in Scope, Management or Operations of THE CA

Severance or merger may result in changes to the scope, management, and/or operations of THE CA. In such an event, the CP and/or the CPS will be modified accordingly.

3.8 Dispute Resolution Process

In the event that a party resorts to resolution mechanisms including legal action or

arbitration against SECOM Trust Systems with regards to usage of THE CA services, the party must contact SECOM Trust Systems in advance.

4. FEES AND CHARGES

THE CA may charge subscribers fees for their use of THE CA's certificate issuing and management services.

5. PUBLICATION AND REPOSITORY REQUIREMENTS

The effective revision of the CPS is normally available in THE CA Repository. Valid certificates and CRLs created by THE CA are published in THE CA Repository. Access to THE CA Repository is normally available to all subscribers and relying parties via Internet.

Access to THE CA Repository is normally available 24 hours a day and 365 days a year to all subscribers and relying parties, except for the case that it is unavailable temporarily when the need of maintenance or any necessary reasons.

6. COMPLIANCE AUDIT REQUIREMENTS

SECOM Trust Systems will maintain THE CA in continual compliance with the "WebTrust for Certification Authorities" program of the AICPA. Topics covered by the WebTrust for Certification Authorities program include:

- Need for business and information practices disclosure
- Maintenance of service integrity
- Maintenance of environmental controls

Should corrections be identified by an audit process, THE CA Personnel will perform all necessary corrective actions as quickly as practicable to bring THE CA certification infrastructure and/or operations into complete compliance with the principles of the WebTrust for Certification Authorities program.

The audit report for WebTrust for CA issued on THE CA may normally be available for inspection by the subscribers in connection with their evaluation of the services.

7. ROOT KEY PAIR GENERATION

7.1 Key Sizes

The Signing key pair of THE CA is 1024 bit, using the RSA algorithm.

7.2 Key Generation Algorithms

THE CA uses the RSA algorithm to generate key pairs.

7.3 Hardware and Software Used for Key Generation

THE CA exclusively uses cryptographic hardware for key generation. The module is compliant to at least FIPS 140-1 level 3.

7.4 Key Usage Purposes

The private key component of THE CA key pair is normally used exclusively to sign certificates issued to a CA and CRLs.

7.5 Key Lifetimes

The intended lifetime of THE CA signing key is twenty years.

8. ROOT PRIVATE KEY PROTECTION

8.1 Key Storage Standards

THE CA signing key is stored exclusively in cryptographic equipment certified to FIPS 140-1 Level 3.

8.2 Key Access

All cryptographic equipment used by THE CA is subject to both physical and logical access control.
More than one personnel is needed to physically access any item of cryptographic equipment.

8.3 Key Escrow

Key pairs generated by THE CA are not escrowed by SECOM Trust Systems or with a third party.

8.4 Key Backup

The signing key of THE CA is stored on both an “operational” item of cryptographic equipment and on a “backup” item of cryptographic equipment. The backup cryptographic equipment may be stored at the outside of main location.

8.5 Key Archival

Expired (and revoked) certificates and any revocation notices on superceded CRLs issued by THE CA may be archived. Archived information is not normally accessible to subscribers and relying-parties.

9. DISTRIBUTION OF ROOT PUBLIC KEYS

9.1 Methods Used

The public keys of the CAs conforming THE CA are delivered to THE CA subscribers according to the rules of the relevant CP.

9.2 Changeover Procedures

The signing keys of the Root CA as managed by THE CA have an intended lifetime of twenty years and the corresponding public key certificates have a lifetime of twenty years.

Upon the end of the lifetime of each signing key of a Root CA managed by THE CA, a new signing key is generated and all subsequently issued certificates and CRLs are signed with the new signing key.

The changed public keys of the Root CAs managed by THE CA are delivered to subscribers according to the relevant CP.

10. ENVIRONMENTAL CONTROLS

10.1 CP and CPS Administration

10.1.1 Non-trivial Changes

Upon changing this CPS, if the SECOM Trust Systems CA Service Improvement Committee determines that proposed changes to this CPS will likely affect Subscriber and/or certificate and/or CRL usage, the committee will update the major version number and notify Subscribers and relying party of the proposed changes. Unless the proposed changes are withdrawn, the proposed changes shall become effective fourteen (14) days after being published.

10.1.2 Trivial Changes

Upon changing this CPS, if the SECOM Trust Systems CA Service Improvement Committee determines that proposed changes to this CPS will not affect Subscriber and/or certificate and/or CRL usage, the committee may update the minor version number and implement the changes without notifying Subscribers or relying party.

10.1.3 Publication and Notification Procedure

Non-trivial changes to this CPS and the effective date shall be notified to Subscribers and relying party via the homepage. Subscribers shall be entitled to provide comments concerning proposed changes within fourteen (14) days of publication. Unless there are comments provided within fourteen (14) days from publication, the proposed changes shall become effective.

10.2 Termination of THE CA

THE CA can only be terminated under the authority of the CA Service Improvement Committee of SECOM Trust Systems.

In the event THE CA is terminated:

- All certificates issued by THE CA will be revoked and THE CA will cease to issue certificates.
- THE CA will provide no less than one month notice to Subscribers that termination is pending.
- The records of THE CA will be archived by SECOM Trust Systems.

10.3 Handling of Confidential, Private and Non-Confidential Information

As THE CA, SECOM Trust Systems shall keep any information it possesses about an individual or organization confidential and private except for information that is

explicitly disclosed as part of a certificate, this CPS or associated CP. SECOM Trust Systems shall not disclose such information externally without due legal reason or previous consent in writing from the appropriate individual or Subscriber. SECOM Trust Systems may disclose such information as part of a non-disclosure agreement with legal or financial advisors for legal, judicial or government procedures or other procedures as required by law. SECOM Trust Systems may also disclose such information as part of a non-disclosure agreement with lawyers, accountants, financial institutions or other advisors as required in the event of a corporate merger, acquisition or restructuring.

The results of security audits may be kept confidential by THE CA, notwithstanding public reporting standards. THE CA does not disclose the results externally without due legal reasons. WebTrust For CA reports maintained by the AICPA may be available via AICPA website.

When THE CA revokes a certificate, if any revocation reason or revocation date may be included in the CRL entry for the revoked certificate, then they are not considered personal and/or private subscriber information and can be shared with all other subscribers and relying parties along with the serial number of the revoked certificate. The other information regarding the certificate revocation is normally not disclosed.

THE CA will comply with legal actions requiring the release of information to law enforcement officials operating in any recognized jurisdiction.

10.4 Intellectual Property Rights

Public key certificates and CRLs issued by THE CA are the property of SECOM Trust Systems. The CPS and associated CP are the property of SECOM Trust Systems.

10.5 Physical Security

THE CA Computer System and THE CA Repository Computer System are used to perform THE CA operations and provide access to THE CA Repository. THE CA Computer System stands alone from all other computer systems and is physically separated from other information systems operated by SECOM Trust Systems. THE CA Repository Computer System is connected to the Internet. Both computer systems are housed in a physically secure facility.

Access to either THE CA Computer System or THE CA Repository Computer System is strictly controlled by the physical security mechanisms of a particular closed area in which it is stored or operated. Only trustworthy operators with a valid business reason are provided access to a closed area. The physical access control system for a closed area

is always functional and uses IC cards or biometric readers to authenticate individual access.

THE CA Computer System and THE CA Repository Computer System benefit from fixing the temperature and humidity by air conditioning systems to provide a suitable operating environment for the equipment and operators.

THE CA has taken reasonable precautions to minimize the impact of water exposure in the facility that houses THE CA Computer System and THE CA Repository Computer System.

THE CA computer systems and THE CA Repository systems are placed in the facility with the appropriate prevention and protection mechanisms against power failure and the earthquake.

Backup media storage for THE CA Computer System and THE CA Repository Computer System is protected such as using tamper-evidenced bags. Also they are stored in a secure manner that more than one personnel is needed to access physically.

Sensitive paper materials relating to THE CA that are designated as waste are normally disposed of by shredding or incineration.

Any electronic records used by THE CA is initialized and, if necessary, physically destroyed before disposal. Any items of cryptographic equipment used by THE CA are initialized and, if necessary, physically destroyed before disposal. The information of THE CA computer systems is disposed by deleting the files.

10.6 Business Continuity Plans

Under the SECOM Trust Systems Security Policy, which contains a business continuity policy, the disaster recovery plan to restore the computer-related elements of THE CA is established. The main purpose of the plan is that a critical business operations to identify the problems is clearly described so that the service be provided in a reasonably timely manner following interruption to, or failure of critical processes.

THE CA Computer System can be reconstructed promptly from system operations data that is stored on media at the outside of the main location.

THE CA Repository Computer System is primarily responsible for publishing certificates, CRLs and CPS. THE CA Repository Computer System can be reconstructed from backup system operations data. Subscribers may be able to get information about

THE CA Repository by contacting THE CA in the event that THE CA Repository Computer System is subject to disaster recovery. The file system on THE CA Repository Computer System is subject to periodic backup.

10.7 Records and Audit Trails

THE CA Personnel may use electronic audit trails or manual procedure for audit trail generation and event logging for THE CA Computer System, THE CA Repository Computer System and associated network devices.

11. CERTIFICATE POLICY

This Certificate Policy (CP) provides notice to all persons who use or rely on certificates issued by “SECOM Trust Systems CA (THE CA)”, a service of SECOM Trust Systems. SECOM Trust Systems has established a certification authority service to issue and manage digital certificates in support of Subscribers' activities such as digital signature or identity authentication.

This CP controls the issuing and management of CA certificates issued to subscribers who wish to issue certificates that chain to THE CA as Root CA.

11.1 Policy-Specific Certification Practices

11.1.1 Subscriber Type

This certificate policy governs THE CA’s issuing and management service intended for Subscribers.

A Subscriber is THE CA customer who may operate one or more levels of subordinate CA below one of the CA conforming THE CA.

11.1.2 Subscriber Naming

The names of subjects of Subscribers must be meaningful. Subscribers may apply their name using the following alphabets, figures and /or symbols; THE CA assigns the applied name as a name of subject if THE CA finds no contradictory to use it.

A ～ Z 、a ～ z 0 ～ 9 ‐ . , _ 0 and 'BLANK'

11.1.3 Method of Confirming Identity

THE CA Personnel identify and authenticate a Subscriber by confirming organizational identity by the identification information sent to THE CA. Also the information source is tested and confirmed that it is from the Subscriber.

11.1.4 CA public key distribution

The public keys of the CAs conforming THE CA are delivered to Subscribers and all relying parties using trusted software distribution and download techniques provided by Microsoft Windows, Linux, etc., and via THE CA Repository.

11.1.5 Subscriber Key Management

THE CA provides no subscriber key management services to Subscribers.

11.1.6 Certificate Publication upon Acceptance

Certificates issued to Subscribers are published to THE CA Repository, shortly in general, after acceptance by the subscriber or making them valid.

11.1.7 Subscriber Revocation Requests

Subscribers may request that THE CA revoke their own certificates by communicating the request to THE CA Personnel, who has knowledge of the representative and who uses this knowledge to test and confirm the identity and authorization of the individual to make the request.

11.2 Policy-Specific Certificate Life Cycle Management

11.2.1 Certificate Profile

THE CA issues certificate whose format complies with the current X.509 standard. No compliance with any other standard, or a profile of standard, should be assumed. In general, THE CA certificates issued to Subscribers are populated with fields that are consistent with those expected in common practice by consumer security platforms such as “Microsoft Windows”, “Apple Macintosh” and “Linux”. Certificates issued after August 1st 2003 use monotonically increasing serial numbers.

11.2.2 Initial Registration

THE CA assigns names to Subscribers from a single name space utilizing the X.500 Distinguished Name form (“THE CA name space”).

All Subscribers of THE CA are unambiguously identified in THE CA name space.

Generally, an obvious variant of the legal name of Subscribers is used by THE CA. Each certificate issued by THE CA is unambiguously identified with the use of Distinguished Name (DN).

Third-party trademarks and related naming issues should not apply to certificates issued within this space by the Subscribers.

Subscriber’s possession of a private key is proved by the applicant demonstrating that he or she holds the private key corresponding to the public key, without disclosing the private key by digitally signing a piece of data with the private key, with the digital signature then being verified by THE CA prior to certificate issuance.

In submitting a certificate application, the Subscriber must provide the following information to THE CA: subscriber’s public key, and subscriber’s requested legal

name(s).
THE CA Personnel check all certification instructions for obvious errors or omissions, only.

11.2.3 External Registration Authorities
THE CA does not use external Registration Authorities. All registration functions are performed by THE CA Personnel.

11.2.4 Certificate Issuance
Certificates are issued to Subscribers upon successful processing of the application.

Certificate format version, validity period, extension fields, and key usage extension field requirements are determine on a case-by-case basis by THE CA. The Subscriber and THE CA agree on these technical parameters before issuing a certificate to the Subscriber.

11.2.5 Certificate Acceptance
Once a certificate has been issued to a Subscriber, it is maintained in a secure manner until it is communicated to the Subscriber for possible acceptance. A Certificate issued to a Subscriber is published to THE CA Repository upon acceptance of the certificate by the Subscriber.

11.2.6 Certificate Distribution
THE CA maintains THE CA Repository for use by subscribers and relying parties. All certificates issued by THE CA to Subscribers and all non-superceded CRLs relating thereto, are published in THE CA Repository.

11.2.7 Certificate ReIssuance/Renewal and Certificate Issuance by rekey
The certificate reissuance/renewal and issuance by rekey is the same process as the initial issuance process for a new certificate.

11.2.8 Certificate Suspension
THE CA does not support suspension of a Subscriber's certificate.

11.2.9 Certificate Revocation
A Subscriber's certificate can be revoked for several reasons including suspected or actual compromise of control of the private key that relates to the public key contained in the certificate, hardware or software failures that render the private key inoperable, or failure of the subscriber to meet the his or her obligations.

Revocation may be requested by the Subscriber. A request by a Subscriber to revoke his or her own certificate must be communicated by the Subscriber in person to THE CA Personnel, who shall employ reasonable precautions to determine the authorization of the individual to make the request. Alternatively, certificate revocation requests may be made via email to root1-support@secomtrust.net. All such requests are processed on a periodic basis by THE CA after the validity of such requests is ascertained. Certificate revocation requests will be validated within 72 hours after receipt. Valid certificate revocation requests will be processed within 7 days of receipt. The certificate may be revoked by THE CA at THE CA's sole discretion, such as failure of the subscriber to meet the his or her obligations.

Revocation requests by a Subscriber for reasons other than key compromise must be placed with THE CA within a maximum of forty-eight hours of the event necessitating revocation. In the case of suspected or known private key compromise, a Subscriber must place a revocation request immediately upon identification of the event.

THE CA's certificate revocation process supports the validation of the source of a revocation request and provides a means of rapid communication of the revocation of a valid certificate by THE CA through the issuance of and publication of an updated CRL. Upon the revocation of a Subscriber's certificate, the newly revoked certificate is recorded in the next CRL that is issued.

11.2.10 Certificate Revocation List Profile

THE CA issues CRLs that comply with the X.509 certificate format. In general, THE CA CRLs are populated with fields that are consistent with those expected in common practice by consumer security platforms such as Microsoft Windows, Apple Macintosh and Linux.

11.2.11 Certificate Status Information

THE CA issues CRLs annually or in the event that THE CA issue or revoke certificates and that THE CA Personnel deem it necessary.

CRL checking is required for all subscribers and relying parties.

THE CA Repository archives all expired certificates and superceded CRLs issued by THE CA.

Acronyms and Definitions

C

CA

Stands for Certification Authority.. An authority trusted by one or more users to create and assign public key certificates. It is important to note that the CA is responsible for the public key certificates during their whole lifetime, not just for issuing them.

Certificate

Digital certificate. It usually refer to a public key certificate, which proves that the public key holder is the one who he/she is by checking the signature of the issuer (CA) signature.

CP

Stands for Certificate Policy. A named set of rules that indicates the applicability of a public key certificate to a particular community or class of application with common security requirements.

CPS

Stands for Certification Practice Statement. A statement of the practices which a CA employs in issuing public key certificates.

CRL

Stands for Certificate Revocation List. It includes the list of all certificates issued and revoked by the issuing CA.

CSR

Stands for Certificate Signing Request. It is the original data sent by the subscriber and CA will issue the certificate using this data, including the public key of the subscriber created by the subscriber.

D

Digital Signature

It proves that a person is the one who create the document with digitally signed data attached.

I

ISMS
Stands for Information Security Management System. An information security management system conformity evaluation system is a third person conformity evaluation system for management of information security in Japan, equivalent to BS7799.

K

Key pair
It consist of the private key and the public key in the public key cryptographic system.

M

Major Version Number
The version number of the CPS in the event of a major update to the CPS. Major updates are defined as changes to the CPS that will likely affect Subscriber and/or User certificate and/or CRL usage. For example, if the CPS version is 1.02, (1) is the major version number.

Minor Version Number
The version number of the CPS in the event of a minor update to the CPS. Minor updates are defined as changes to the CPS that will not affect Subscriber and/or User certificate and/or CRL usage. For example, if the CPS version is 1.02, (02) is the minor version number.

P

Private Key
One of the key pair in the public key cryptographic system, normally the one only subscriber is able to hold and access.

Public Key
One of the key pair in the public key cryptographic system, normally the one available to the public.

R

Registration Authority (RA)

An optional entity given responsibility for performing some of the administrative tasks necessary in the registration of subjects, such as: confirming the subject's identity.

Relying Party

A user or agent (e.g., a client or server) who relies on the data in a certificate in making decisions.

Repository

The storage site for certificates issued by the CA. The repository is a mechanism that allows users and applications to access certificates from anywhere on the network. The CRL and CPS are stored in the repository as well.

Root CA

SECOM Trust.net Root1 CA will issue and sign the public key certificate to a subordinate CA as a Root CA operated by SECOM Trust Systems Co.,Ltd. Root CA is the top of the trusted chain in a domain.

S

SECOM Trust Systems CA Service Improvement Committee

The organization responsible for the management and updating of the CPS and verification of service operation.

Subordinate CA

Not a Root CA. SECOM Trust.net Root1 CA will issue and sign the public key certificate to a subordinate CA, which holds the private key corresponding to it.

Subscriber

Meaning a subordinate CA to which THE CA issues certificates.

W

Webtrust for CA

Developed by AICPA and CICA, it is the standard and an authorization system over the standard for the internal control about the reliability of a certificate authority (CA), the safety of electronic commerce, etc.

X

X.500

Directory Standard defined by ITU-T for the purpose of name and address search and/or retrieving the attributes. X.500 Distinguished Name is used for the issuer and subject name.

X.509

The format of a digital certificate and a certificate revocation list defined by ITU-T. In X.509 version3, the extension for information used by issuers is added.