



あずさ監査法人

有限責任 あずさ監査法人

〒162-8551

東京都新宿区津久戸町 1 番 2 号

あずさセンタービル

Telephone 03 3266 7500

Fax 03 3266 7600

Internet home.kpmg/jp/azsa

独立業務実施者の保証報告書

2023 年 8 月 24 日

セコムトラストシステムズ株式会社

執行役員 梶澤 慎之助 殿

有限責任 あずさ監査法人

東京事務所

パートナー 公認会計士

紫垣昌利

範囲

当監査法人は、[認証局のための WebTrust の規準 v2.2.2 \(the WebTrust Principles and Criteria for Certification Authorities v2.2.2\)](#) に準拠して、2023 年 2 月 24 日から 2023 年 6 月 6 日までの期間において、[付録 A](#) に記載されたセコムトラストシステムズ株式会社の認証局（以下「CA」という。）のサービス（東京）（以下「CA サービス」という。）に関する[経営者の記述書](#)について合理的保証業務を行った。

経営者の記述書によれば、セコムトラストシステムズ株式会社は CA サービスについて、下記事項を実施していた。

1. セコムトラストシステムズ株式会社は、CA が実施するビジネス、鍵のライフサイクル管理と証明書のライフサイクル管理及び CA 環境の内部統制の実務を、セコムトラストシステムズ株式会社のウェブサイトで[付録 B](#) に記載された認証局運用規程及び証明書ポリシーにて開示していた。
2. セコムトラストシステムズ株式会社は、下記について合理的な保証を提供する有効な内部統制を維持していた。
 - ・ セコムトラストシステムズ株式会社の認証局運用規程は、証明書ポリシーと整合していたこと。
 - ・ セコムトラストシステムズ株式会社は、証明書ポリシー及び認証局運用規程に準拠してサービスを提供していたこと。
3. セコムトラストシステムズ株式会社は、下記について合理的な保証を提供する有効な内部統制を維持していた。
 - ・ セコムトラストシステムズ株式会社が管理する鍵と証明書のインテグリティが確立され、そのライフサイクルを通じて保護されていたこと。
 - ・ セコムトラストシステムズ株式会社が管理する加入者鍵及び加入者証明書のインテグリティが確立され、そのライフサイクルを通じて保護されていたこと。

- ・ 加入者の情報は、（セコムトラストシステムズ株式会社が行う登録業務のため）適切に認証されていたこと。
- ・ 下位CAの証明書申請は、正確で、認証され、承認されていたこと。

4. セコムトラストシステムズ株式会社は、下記について合理的な保証を提供する有効な内部統制を維持していた。

- ・ CA システム及びデータへの論理的、物理的アクセスは、承認された個人に制限されていたこと。
- ・ 鍵と証明書の管理に関する運用の継続性が維持されていたこと。
- ・ CA システムのインテグリティを維持するため、CA システムの開発、保守及び運用が適切に承認され、実施されていたこと。

セコムトラストシステムズ株式会社は、CA の鍵を寄託せず、証明書の一時的停止サービスを提供しない。従って、当監査法人の手続は、それらの規準に関連する内部統制を含んでいない。

認証局の責任

セコムトラストシステムズ株式会社の経営者の責任は、[認証局のための WebTrust の規準 v2.2.2](#) に準拠して、経営者の記述書を適正に作成すること、及び、記述書に記載されたサービスを提供することにある。

職業倫理、独立性及び品質管理

当監査法人は、誠実性、客観性、職業的専門家としての能力及び正当な注意、守秘義務及び職業的専門家としての行動に関する基本原則を基礎とする国際会計士倫理基準審議会の職業会計士のための国際倫理規程（国際独立性基準を含む。）（国際倫理規程）の独立性及びその他の職業倫理に関する規定を遵守した。

また、当監査法人は、国際品質マネジメント基準第1号を適用しており、これは、職業倫理に関する規定、職業的専門家としての基準及び適用される法令等の要求事項の遵守に関する方針と手続を含む、品質マネジメントシステムをデザイン、適用及び運用することを要求している。

業務実施者の責任

当監査法人の責任は、当監査法人の実施した手続に基づいて経営者の記述書に対して意見を表明することにある。

当監査法人は、国際監査・保証基準審議会が公表した国際保証業務基準 3000「過去財務情報の監査又はレビュー以外の保証業務」に準拠して業務を実施した。当該指針は、当監査法人に、すべての重要な点において、経営者の記述書が適正に表示されているかどうかについて、合理的な保証を得るための手続を計画し実施することを求めている。従って、手続には、(1) セコムトラストシステムズ株式会社の鍵と証明書のライフサイクル管理のビジネス実務及び鍵と証明書のインテグリティ、加入者と信頼者情報の認証と機密保持、鍵と証明書のライフサイクル管理に係る運用の継続性、システムインテグリティの開発、保守、及び運用に関する内部統制を理解すること、(2) セコムトラストシステムズ株式会社が開示した鍵と証明書のライフサイクル管理のビジネス実務に従って実施された取引を試査によりテストすること、(3) 内部統制の運用評価手続を実施し評価すること、(4) 当監査法人が状況に応じて必要と認めたその他の手続を実施することを含んでいる。

当監査法人は、意見表明の基礎となる十分かつ適切な証拠を入手したと判断している。



セコムトラストシステムズ株式会社における特定の内部統制の相対的な有効性と重要性、及び加入者と信頼者の内部統制リスクの評価に与える影響は、内部統制との相互作用、及び個々の加入者と信頼者の所在場所において現れるその他の要因に依存している。当監査法人は個別の加入者と信頼者の所在場所における内部統制の有効性を評価するための手続を実施していない。

内部統制の限界

内部統制の有効性には、人為的なミスの可能性や内部統制の回避など、固有の限界がある。例えば、その性質により、内部統制は、システムや情報への未承認のアクセス、社内及び外部のポリシーや要求への遵守性違反を防止、発見することができないことがある。又、当監査法人の発見事項に基づく結論の将来への予測は、内部統制が無効になる可能性があるというリスクの影響を受ける。

意見

当監査法人は、セコムトラストシステムズ株式会社の経営者の記述書が、[認証局のための WebTrust の規準 v2.2.2](#)に基づいて、2023 年 2 月 24 日から 2023 年 6 月 6 日までの期間において、すべての重要な点において適正に表示されているものと認める。

この保証報告書は、[認証局のための WebTrust の規準 v2.2.2](#)が対象としている範囲を超えて、セコムトラストシステムズ株式会社のサービスの品質について何ら表明するものではない。また、いかなる顧客の意図する目的に対するセコムトラストシステムズ株式会社のサービスの適合性についても何ら表明するものではない。

WebTrust シールの使用

セコムトラストシステムズ株式会社の認証局のための WebTrust シールの使用は、この保証報告書の内容を象徴的に表示しているが、この保証報告書の変更又は追加的な保証を提供することを意図したものではなく、そのような解釈をすべきではない。

以上



付録 A

対象 CA

Root Cas
CA#1: SECOM RSA Root CA 2023
CA#2: SECOM Document Signing RSA Root CA 2023
Document Signing Cas
CA#3: SECOM Passport for PublicID AATL RSA CA 2023
Timestamp Cas
CA#4: SECOM TimeStamping CA4



対象CAの識別情報

CA #	Cert #	サブジェクト	発行者	シリアル番号	キーアルゴリズム	キーサイズ	ダイジェストアルゴリズム	有効期限の開始	有効期限の終了	サブジェクト キー識別子	拇印
1	1	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	99B8098D4418 DDDB	rsaEncryption	4096bit	sha384WithRSAEncryption	Jan 25 08:03:37 2023 GMT	Jan 1 08:03:37 2048 GMT	51336A2AEFDB1F80E2C154235528D701790B675AFF6E1970827B10ED665E913835BF46E3460FD5C84C8B666	
2	1	CN = SECOM Document Signing RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP-4011001040781 C = JP	CN = SECOM Document Signing RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP-4011001040781 C = JP	E3A2A1C4FE81A10D	rsaEncryption	4096bit	sha384WithRSAEncryption	Jan 25 08:33:59 2023 GMT	Jan 1 08:33:59 2048 GMT	01DDB12430892CC803835E10AE711E49F2EE4B07	46219BBF9148F00E8B7A4C619B57CF7602701FF81348400718870FABD31FC5BE
3	1	CN = SECOM Passport for PublicID AATL RSA CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP-4011001040781 C = JP	CN = SECOM Document Signing RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP-4011001040781 C = JP	010000065E566F5039F9576061C0FD6F	rsaEncryption	4096bit	sha384WithRSAEncryption	Feb 24 07:41:36 2023 GMT	Feb 1 00:00:00 2043 GMT	8939416491E946A4165907F22BAF527F7D4BDA92	D2A60B7C6DFE267AD055DA26BF68D9F1478D862310F3DD0A73325941C2F00DD E
4	1	CN = SECOM TimeStamping CA4 O = SECOM Trust Systems CO.,LTD. C = JP	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	010000057397549EA8FB9F7ED5DD6EEC	rsaEncryption	4096bit	sha384WithRSAEncryption	Feb 24 07:12:49 2023 GMT	Feb 1 00:00:00 2043 GMT	60811F0DE823DC6EB9B7A75CCF8D0EDAC6088D40F14B6D20C85C69B2B7F5A2C957FB1C2BC5870BAF01949BEE7F90D2448C19DB65	



付録 B

証明書ポリシー

CA	CP 名	Version	日付
CA#1	Security Communication RootCA 下位 CA 用証明書ポリシー	6.02	2023/5/17
CA#2	Security Communication RootCA 下位 CA 用証明書ポリシー	6.01	2023/2/10
CA#1	Security Communication RootCA タイムスタンプサービス用証明書ポリシー	5.08	2023/5/17
CA#2	Security Communication RootCA タイムスタンプサービス用証明書ポリシー	5.07	2022/12/8
CA#3	セコムパスポート for Member 2.0 PUB 証明書ポリシー	6.04	2023/5/17
	セコムパスポート for Member 2.0 PUB 証明書ポリシー	6.03	2023/2/17
CA#4	SECOM TimeStamping CA タイムスタンプサービス用証明書ポリシー	5.05	2023/5/17
	SECOM TimeStamping CA タイムスタンプサービス用証明書ポリシー	5.04	2023/2/17

運用規程

CA	CPS 名	Version	日付
CA#1	Security Communication RootCA 認証運用規定	6.02	2023/5/17
CA#2	Security Communication RootCA 認証運用規定	6.01	2023/2/10
CA#3	セコム電子認証基盤認証運用規程 (Certification Practice Statement)	2.18	2023/5/17
CA#4	セコム電子認証基盤認証運用規程 (Certification Practice Statement)	2.17	2022/12/8

経営者の記述書

2023 年 8 月 24 日

セコムトラストシステムズ株式会社

執行役員

花岡 慎之助

当社は、[付録 A](#)に記載された認証局（以下「CA」という。）を運営し、次の認証局サービス（以下「CA サービス」という。）を提供している。

- ・ 加入者の登録
- ・ 証明書の更新
- ・ 証明書の再生成
- ・ 証明書の発行
- ・ 証明書の配送
- ・ 証明書の失効
- ・ 証明書の審査
- ・ 加入者鍵の生成と管理
- ・ 下位 CA の相互認証

当社の経営者は、当社の Web サイトで公開している CA ビジネス実務の開示、CA ビジネス実務の管理、CA 環境の内部統制、CA 鍵のライフサイクル管理の内部統制、加入者鍵ライフサイクル管理の内部統制、証明書のライフサイクル管理の内部統制、及び下位 CA の証明書ライフサイクル管理の内部統制を含む当社の CA の運用について、有効な内部統制を確立し、維持することに責任がある。これらの内部統制はモニタリングの仕組みを含んでおり、識別された欠陥を修正するための行動が取られる。

内部統制には、人為的なミスの可能性や内部統制の回避など、固有の限界がある。従って、有効な内部統制といえども、当社の CA の運用について合理的な保証を提供するものでしかない。さらに、状況の変化により、内部統制の有効性は時間とともに変化する可能性がある。

当社の経営者は、当社の CA（東京）の運用に関するビジネス実務の開示と内部統制を評価した。その評価に基づく当社の経営者の意見では、当社は、[認証局のための WebTrust の規準 v2.2.2\(the WebTrust Principles and Criteria for Certification Authorities](#)

[v2.2.2](#)に準拠して、2023年2月24日から2023年6月6日までの期間において、CAサービスの提供に関して、下記の事項を実施した。

1. 当社のCAが実施するビジネス、鍵のライフサイクル管理と証明書のライフサイクル管理及びCA環境の内部統制の実務を、当社のWebサイトで[付録B](#)に記載された認証局運用規程及び証明書ポリシーにて開示していた。
2. 下記について合理的な保証を提供するための有効な内部統制を維持していた。
 - ・ 当社の証明書ポリシーと認証局運用規程が整合していたこと。
 - ・ 当社は、証明書ポリシー及び認証局運用規程に準拠してサービスを提供していたこと。
3. 下記について合理的な保証を提供するための有効な内部統制を維持していた。
 - ・ 当社が管理する鍵と証明書のインテグリティが確立され、そのライフサイクルを通じて保護されていたこと。
 - ・ 当社が管理する加入者鍵と加入者証明書のインテグリティが確立され、そのライフサイクルを通じて保護されていたこと。
 - ・ 加入者の情報は、（当社が行う登録業務のため）適切に認証されていたこと。
 - ・ 下位CAの証明書申請は、正確で、認証され、承認されていたこと。
4. 下記について合理的な保証を提供するための有効な内部統制を維持していた。
 - ・ CAシステムとデータへの論理的、物理的アクセスは、承認された個人に制限されていたこと。
 - ・ 鍵と証明書の管理に関する運用の継続性が維持されていたこと。
 - ・ CAシステムのインテグリティを維持するため、CAシステムの開発、保守及び運用が適切に承認され、実施されていたこと。

当社が準拠した[認証局のための WebTrust の規準 v2.2.2](#)には、以下が含まれる。

CA ビジネス実務の開示

- ・ 認証局運用規程（CPS）
- ・ 証明書ポリシー（CP）

CA のビジネス実務管理

- ・ 証明書ポリシー管理
- ・ 認証局運用規程の管理
- ・ CP および CPS の一貫性

CA 環境の内部統制

- ・ セキュリティ管理
- ・ 資産の分類と管理
- ・ 人員のセキュリティ
- ・ 物理的・環境的セキュリティ
- ・ 運用管理
- ・ システムアクセス管理
- ・ システム開発と保守
- ・ ビジネス継続性の管理
- ・ モニタリングと遵守
- ・ 監査ログの取得

CA 鍵ライフサイクル管理の内部統制

- ・ CA 鍵の生成
- ・ CA 鍵のストレージ、バックアップと復旧
- ・ CA 公開鍵の配送
- ・ CA 鍵の使用法
- ・ CA 鍵の保存及び破壊
- ・ CA 鍵の危殆化
- ・ CA の暗号化ハードウェアライフサイクルの管理

加入者鍵ライフサイクル管理の内部統制

- ・ CA が提供する加入者鍵生成サービス
- ・ CA が提供する鍵保存及び復旧サービス
- ・ IC カードライフサイクル管理
- ・ 加入者鍵管理の要件

証明書ライフサイクル管理の内部統制

- ・ 加入者の登録
- ・ 証明書の更新
- ・ 証明書の再生成
- ・ 証明書の発行
- ・ 証明書の配送
- ・ 証明書の失効
- ・ 証明書の審査

下位 CA の証明書ライフサイクル管理の内部統制

- ・ 下位 CA 証明書ライフサイクル管理

当社は、CA の鍵を寄託せず、証明書の一時的停止サービスを提供しない。従って、当社の記述書には、それらの規準に関連する内部統制を含んでいない。

付録 A

対象CA

Root Cas
CA#1: SECOM RSA Root CA 2023
CA#2: SECOM Document Signing RSA Root CA 2023
Document Signing Cas
CA#3: SECOM Passport for PublicID AATL RSA CA 2023
Timestamp Cas
CA#4: SECOM TimeStamping CA4

対象 CA の識別情報

CA #	Cert #	サブジェクト	発行者	シリアル番号	キーアルゴリズム	キーサイズ	ダイジェストアルゴリズム	有効期限の開始	有効期限の終了	サブジェクト キー識別子	拇印
1	1	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	99B8098D4418DDDB	rsaEncryption	4096bit	sha384WithRSAEncryption	Jan 25 08:03:37 2023 GMT	Jan 1 08:03:37 2048 GMT	51336A2AEFDB1F80E2C154235528D701790B675AFF6E1970827B10ED665E913835BF46E3460FD5C84DB2C6D306D22593C4C8B666	
2	1	CN = SECOM Document Signing RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP-4011001040781 C = JP	CN = SECOM Document Signing RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP-4011001040781 C = JP	E3A2A1C4FE81A10D	rsaEncryption	4096bit	sha384WithRSAEncryption	Jan 25 08:33:59 2023 GMT	Jan 1 08:33:59 2048 GMT	01DDB12430892CC803835E10AE711E49F2EE4B07	46219BBF9148F00E8B7A4C619B57CF7602701FF81348400718870FABD31FC5BE
3	1	CN = SECOM Passport for PublicID AATL RSA CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP-4011001040781 C = JP	CN = SECOM Document Signing RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP-4011001040781 C = JP	010000065E566F5039F9576061C0FD6F	rsaEncryption	4096bit	sha384WithRSAEncryption	Feb 24 07:41:36 2023 GMT	Feb 1 00:00:00 2043 GMT	8939416491E946A4165907F22BAF527F7D4BDA92	D2A60B7C6DFE267AD055DA26BF68D9F1478D862310F3DD0A73325941C2F00DD
4	1	CN = SECOM TimeStamping CA4 O = SECOM Trust Systems CO.,LTD. C = JP	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	010000057397549EA8FB9F7ED5DD6EEC	rsaEncryption	4096bit	sha384WithRSAEncryption	Feb 24 07:12:49 2023 GMT	Feb 1 00:00:00 2043 GMT	60811F0DE823DC6EB9B7A75CCF8D0EDAC6088D40F14B6D20C85C69B2B7F5A2C957FB1C2BC5870BAF01949BEE7F90D2448C19DB6	5

付録 B

証明書ポリシー

CA	CP 名	Version	日付
CA#1	Security Communication RootCA 下位 CA 用証明書ポリシー	6.02	2023/5/17
CA#2	Security Communication RootCA 下位 CA 用証明書ポリシー	6.01	2023/2/10
CA#1	Security Communication RootCA タイムスタンプサービス用証明書ポリシー	5.08	2023/5/17
CA#2	Security Communication RootCA タイムスタンプサービス用証明書ポリシー	5.07	2022/12/8
CA#3	セコムパスポート for Member 2.0 PUB 証明書ポリシー	6.04	2023/5/17
	セコムパスポート for Member 2.0 PUB 証明書ポリシー	6.03	2023/2/17
CA#4	SECOM TimeStamping CA タイムスタンプサービス用証明書ポリシー	5.05	2023/5/17
	SECOM TimeStamping CA タイムスタンプサービス用証明書ポリシー	5.04	2023/2/17

運用規程

CA	CPS 名	Version	日付
CA#1	Security Communication RootCA 認証運用規定	6.02	2023/5/17
CA#2	Security Communication RootCA 認証運用規定	6.01	2023/2/10
CA#3	セコム電子認証基盤認証運用規程 (Certification Practice Statement)	2.18	2023/5/17
CA#4	セコム電子認証基盤認証運用規程 (Certification Practice Statement)	2.17	2022/12/8

以上



KPMG AZSA LLC
AZSA Center Building
1-2 Tsukudo-cho, Shinjuku-ku
Tokyo 162-8551, Japan
Telephone +81 (3) 3266 7500
Fax +81 (3) 3266 7600
Internet home.kpmg/jp/azsa

(Translation)

INDEPENDENT ASSURANCE REPORT

August 24, 2023

To Mr. Shinnosuke Kabasawa
Executive Officer
SECOM Trust Systems Co., Ltd.

KPMG AZSA LLC
Tokyo Office
Partner, Certified Public Accountant
Masatoshi Shigaki

Scope

We have been engaged, in a reasonable assurance engagement, to report on the [management's assertion](#) of SECOM Trust Systems Co., Ltd. ("STS") that for its Certification Authority (CA) operations at Tokyo, Japan, throughout the period February 24, 2023 to June 6, 2023 for its CAs as enumerated in [Appendix A](#), STS has:

1. disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statements and Certificate Policies enumerated in [Appendix B](#) on STS website
2. maintained effective controls to provide reasonable assurance that:
 - the Certification Practice Statements of STS are consistent with its Certificate Policies; and
 - STS provides its services in accordance with its Certificate Policies and Certification Practice Statements
3. maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
 - the Subscriber information is properly authenticated (for the registration activities performed by STS); and
 - subordinate CA certificate requests are accurate, authenticated, and approved
4. maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorized individuals;



(Translation)

- the continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

STS does not escrow its CA keys, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.

Certification authority's responsibilities

STS's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

Our independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (including International Independence Standards) (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies International Standard on Quality Management 1 which requires the firm to design, implement and operate a system of quality management including policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

- (1) obtaining an understanding of STS's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations, and over the development, maintenance and operation of systems integrity;
- (2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
- (3) testing and evaluating the operating effectiveness of the controls; and
- (4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.



(Translation)

The relative effectiveness and significance of specific controls at STS and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, throughout the period February 24, 2023 to June 6, 2023, STS management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

This report does not include any representation as to the quality of STS's services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#), nor the suitability of any of STS's services for any customer's intended purpose.

Use of the WebTrust seal

STS's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

(The above represents a translation, for convenience only, of the original report issued in the Japanese language.)



(Translation)

APPENDIX A

List of CAs in Scope

Root Cas
CA#1: SECOM RSA Root CA 2023
CA#2: SECOM Document Signing RSA Root CA 2023
Document Signing Cas
CA#3: SECOM Passport for PublicID AATL RSA CA 2023
Timestamp Cas
CA#4: SECOM TimeStamping CA4



(Translation)

CA Identifying Information for in Scope CAs

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	SHA256 Fingerprint
1	1	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	99B8098D4418 DDDB	rsaEncr yption	4096bit	sha384With RSAEncrypt ion	Jan 25 08:03:37 2023 GMT	Jan 1 08:03:37 2048 GMT	51336A2AEFDB1F80E DB2C6D306D22593C4 C8B666	2C154235528D701790B675AFF6E1970827B10ED665E913835BF46E3460FD5C84
2	1	CN = SECOM Document Signing RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP- 4011001040781 C = JP	CN = SECOM Document Signing RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP- 4011001040781 C = JP	E3A2A1C4FE81 A10D	rsaEncr yption	4096bit	sha384With RSAEncrypt ion	Jan 25 08:33:59 2023 GMT	Jan 1 08:33:59 2048 GMT	01DDB12430892CC80 3835E10AE711E49F2 EE4B07	46219BBF9148F00E8B7A4C619B57CF7602701FF81348400718870FABD31FC5BE
3	1	CN = SECOM Passport for PublicID AATL RSA CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP- 4011001040781 C = JP	CN = SECOM Document Signing RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP- 4011001040781 C = JP	010000065E566 F5039F9576061 C0FD6F	rsaEncr yption	4096bit	sha384With RSAEncrypt ion	Feb 24 07:41:36 2023 GMT	Feb 1 00:00:00 2043 GMT	8939416491E946A416 5907F22BAF527F7D4 BDA92	D2A60B7C6DFE267AD055DA26BF68D9F1478D862310F3DD0A73325941C2F00DD E
4	1	CN = SECOM TimeStamping CA4 O = SECOM Trust Systems CO.,LTD. C = JP	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	01000005739754 9EA8FB9F7ED5 DD6EEC	rsaEncr yption	4096bit	sha384With RSAEncrypt ion	Feb 24 07:12:49 2023 GMT	Feb 1 00:00:00 2043 GMT	60811F0DE823DC6EB 01949BEE7F90D2448 C19DB6	9B7A75CCF8D0EDAC6088D40F14B6D20C85C69B2B7F5A2C957FB1C2BC5870BAF 5



(Translation)

APPENDIX B

Certificate Policy

CA	Policy Name	Version	Date
CA#1 CA#2	Security Communication RootCA Subordinate CA Certificate Policy	6.02	May 17, 2023
	Security Communication RootCA Subordinate CA Certificate Policy	6.01	February 10, 2023
CA#1 CA#2	Security Communication RootCA Time-Stamp Service Certificate Policy	5.08	May 17, 2023
	Security Communication RootCA Time-Stamp Service Certificate Policy	5.07	December 8, 2022
CA#3	SECOM Passport for Member 2.0 PUB Certificate Policy	6.04	May 17, 2023
	SECOM Passport for Member 2.0 PUB Certificate Policy	6.03	February 17, 2023
CA#4	SECOM TimeStamping CA Time-Stamp Service Certificate Policy	5.05	May 17, 2023
	SECOM TimeStamping CA Time-Stamp Service Certificate Policy	5.04	February 17, 2023

Certification Practice Statement

CA	Policy Name	Version	Date
CA#1 CA#2	Security Communication RootCA Certification Practice Statement	6.02	May 17, 2023
	Security Communication RootCA Certification Practice Statement	6.01	February 10, 2023
CA#3 CA#4	SECOM Digital Certification Infrastructure Certification Practice Statement	2.18	May 17, 2023
	SECOM Digital Certification Infrastructure Certification Practice Statement	2.17	December 8, 2022

STS MANAGEMENT'S ASSERTION

August 24, 2023

Shinnosuke Kabasawa
Executive Officer
SECOM Trust Systems Co., Ltd.

SECOM Trust Systems Co., Ltd. ("STS") operates the Certification Authority (CA) services for its CAs as enumerated in [Appendix A](#), and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management
- Subordinate CA cross-certification

The management of STS is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to STS's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

STS management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in STS management's opinion, in providing its Certification Authority (CA) services at Tokyo, Japan, throughout the period February 24, 2023 to June 6, 2023, STS has:

1. disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statements and Certificate Policies enumerated in [Appendix B](#) on STS's website
2. maintained effective controls to provide reasonable assurance that:
 - the Certification Practice Statements of STS are consistent with its Certificate Policies; and
 - STS provides its services in accordance with its Certificate Policies and Certification Practice Statements
3. maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
 - subscriber information is properly authenticated (for the registration activities performed by STS); and
 - subordinate CA certificate requests are accurate, authenticated, and approved
4. maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorized individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#), including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services

(Translation)

- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

STS does not escrow its CA keys, and does not provide certificate suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.

(The above represents a translation, for convenience only, of the original assertion issued in the Japanese language.)

APPENDIX A

List of CAs in Scope

Root Cas
CA#1: SECOM RSA Root CA 2023
CA#2: SECOM Document Signing RSA Root CA 2023
Document Signing Cas
CA#3: SECOM Passport for PublicID AATL RSA CA 2023
Timestamp Cas
CA#4: SECOM TimeStamping CA4

(Translation)

CA Identifying Information for in Scope CAs

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	SHA256 Fingerprint
1	1	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	99B8098D4418 DDDB	rsaEncr yption	4096bit	sha384With RSAEncrypt ion	Jan 25 08:03:37 2023 GMT	Jan 1 08:03:37 2048 GMT	51336A2AEFDB1F80E DB2C6D306D22593C4 C8B666	2C154235528D701790B675AFF6E1970827B10ED665E913835BF46E3460FD5C84
2	1	CN = SECOM Document Signing RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP- 4011001040781 C = JP	CN = SECOM Document Signing RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP- 4011001040781 C = JP	E3A2A1C4FE81 A10D	rsaEncr yption	4096bit	sha384With RSAEncrypt ion	Jan 25 08:33:59 2023 GMT	Jan 1 08:33:59 2048 GMT	01DDB12430892CC80 3835E10AE711E49F2 EE4B07	46219BBF9148F00E8B7A4C619B57CF7602701FF81348400718870FABD31FC5BE
3	1	CN = SECOM Passport for PublicID AATL RSA CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP- 4011001040781 C = JP	CN = SECOM Document Signing RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. 2.5.4.97 = NTRJP- 4011001040781 C = JP	010000065E566 F5039F9576061 C0FD6F	rsaEncr yption	4096bit	sha384With RSAEncrypt ion	Feb 24 07:41:36 2023 GMT	Feb 1 00:00:00 2043 GMT	8939416491E946A416 5907F22BAF527F7D4 BDA92	D2A60B7C6DFE267AD055DA26BF68D9F1478D862310F3DD0A73325941C2F00DD
4	1	CN = SECOM TimeStamping CA4 O = SECOM Trust Systems CO.,LTD. C = JP	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	01000005739754 9EA8FB9F7ED5 DD6EEC	rsaEncr yption	4096bit	sha384With RSAEncrypt ion	Feb 24 07:12:49 2023 GMT	Feb 1 00:00:00 2043 GMT	60811F0DE823DC6EB 01949BEE7F90D2448 C19DB6	9B7A75CCF8D0EDAC6088D40F14B6D20C85C69B2B7F5A2C957FB1C2BC5870BAF5

APPENDIX B

Certificate Policy

CA	Policy Name	Version	Date
CA#1 CA#2	Security Communication RootCA Subordinate CA Certificate Policy	6.02	May 17, 2023
	Security Communication RootCA Subordinate CA Certificate Policy	6.01	February 10, 2023
CA#1 CA#2	Security Communication RootCA Time-Stamp Service Certificate Policy	5.08	May 17, 2023
	Security Communication RootCA Time-Stamp Service Certificate Policy	5.07	December 8, 2022
CA#3	SECOM Passport for Member 2.0 PUB Certificate Policy	6.04	May 17, 2023
	SECOM Passport for Member 2.0 PUB Certificate Policy	6.03	February 17, 2023
CA#4	SECOM TimeStamping CA Time-Stamp Service Certificate Policy	5.05	May 17, 2023
	SECOM TimeStamping CA Time-Stamp Service Certificate Policy	5.04	February 17, 2023

Certification Practice Statement

CA	Policy Name	Version	Date
CA#1 CA#2	Security Communication RootCA Certification Practice Statement	6.02	May 17, 2023
	Security Communication RootCA Certification Practice Statement	6.01	February 10, 2023
CA#3 CA#4	SECOM Digital Certification Infrastructure Certification Practice Statement	2.18	May 17, 2023
	SECOM Digital Certification Infrastructure Certification Practice Statement	2.17	December 8, 2022