



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

2024 年 8 月 26 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 6 月 7 日から 2024 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。

- 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。
- 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。
- 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。

付録Aの「対象CAの識別情報」に記載されているCA #1-1は、2023年9月30日に廃止された。

CA #13-2は、2023年11月20日に廃止された。

CA #23-2は、2023年11月11日から2023年11月16日までの期間において、証明書を発行せず、失効ステータス情報のみをオンラインで提供していた。また、2023年11月16日に廃止された。

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、当監査法人の手続きは、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6月7日から2024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。

その他の情報

セコムトラストシステムズ株式会社の経営者は、CA ブラウザフォーラムを構成するインターネットブラウザのオンラインフォーラムである Bugzilla のサイトで公開された情報を記載した[付録 C](#)を当監査法人に開示している。

以上



付録 A

対象 CA

Root CAs
CA#1: Security Communication RootCA1
CA#2: Security Communication RootCA2
CA#3: Security Communication RootCA3
CA#4: Security Communication ECCRootCA1
CA#5: SECOM RSA Root CA 2023
CA#6: SECOM Document Signing RSA Root CA 2023
OV SSL Issuing CAs
CA#7: SECOM Passport for Web SR 3.0 CA
CA#8: NII Open Domain CA - G7 RSA
CA#9: NII Open Domain CA - G7 ECC
CA#10: CrossTrust OV CA5
EV SSL Issuing CAs
CA#11: SECOM Passport for Web EV 2.0 CA
Non-EV Code Signing Issuing CAs
CA#12: SECOM Passport for CodeSigning CA G2
Secure Email (S/MIME) CAs
CA#13: SECOM Passport for Member PUB CA4
CA#14: SECOM Passport for Member PUB CA5
CA#15: SECOM Passport for Member PUB CA8
CA#16: SECOM Passport for PublicID SMIME RSA CA 2023



Document Signing CAs
CA#17: SECOM Passport for Member PUB CA7
CA#18: SECOM Passport for PublicID Document Signing RSA CA 2023
CA#19: SECOM Passport for PublicID AATL RSA CA 2023
CA#20: SMBC Certificate Authority CA2
CA#21: SMBC Certificate Authority CA2 G2
Timestamp CAs
CA#22: SECOM TimeStamping CA3
CA#23: SECOM TimeStamping CA4
CA#24: SECOM TimeStamping CA2
Other CAs
CA#25: CrossTrust DV CA5
CA#26: FujiSSL Public Validation Authority - G3



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	ダイジェスタアルゴリズム	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	ポリシーオブジェクト識別子
1	1	OU = Security Communication RootCA1 O = SECOM Trust.net C = JP	OU = Security Communication RootCA1 O = SECOM Trust.net C = JP	00	rsaEncryption	2048bit	sha1WithRSAEncryption	Sep 30 04:20:49 2003 GMT	Sep 30 04:20:49 2023 GMT	A073499968DC855B65E39B282F579FBD33BC0748	E75E72ED9F560EEC6EB4800073A43FC3AD19195A392282017895974A99026B6C	
2	1	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	00	rsaEncryption	2048bit	sha256WithRSAEncryption	May 29 05:00:39 2009 GMT	May 29 05:00:39 2029 GMT	0A85A9776505987C4081F80F972C38F10AEC3CCF	513B2CECB810D4CDE5DD85391ADFC6C2DD60D87BB736D2B521484AA47A0EBEF6	2.23.140.1.2.1 2.23.140.1.2.2 2.23.140.1.1 2.23.140.1.4.1 2.23.140.1.5.1.3
3	1	OU = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	00E17C3740FD1BFE67	rsaEncryption	4096bit	sha384WithRSAEncryption	Jun 16 06:17:16 2016 GMT	Jan 18 06:17:16 2038 GMT	64147CFC587216A60A2934156F2ACBBCFAFA8AB	24A55C2AB051442D0617766541239A4AD032D7C55175AA34FFDE2FBC4F5C5294	2.23.140.1.4.1 2.23.140.1.4.2
4	1	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	00D65D9BB378812EEB	ECDSAEncryption	384bit	sha384WithECDSAEncryption	Jun 16 05:15:28 2016 GMT	Jan 18 05:15:28 2038 GMT	861CE7FE2DA54A8B08FE2811FABEA366F860592F	E74FBDA55BD564C473A36B441AA799C8A68E077440E8288B9FA1E50E4BBACA11	2.23.140.1.2.1 2.23.140.1.2.2



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	ダイジェスタアルゴリズム	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	ポリシーオブジェクト識別子
4	2	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B1A49DB1D47C2674294CEE84F8FC	ECDSA Encryption	384bit	sha384WithECDSAEncryption	Apr 4 06:22:18 2024 GMT	May 29 05:00:39 2029 GMT	861CE7FE2DA54A8B08FE2811FABEA366F860592F	C3EBCEA7E6B13AC3EB3A79F05819E67D6893C65642F50D9B5E1647CB26506B8E	2.23.140.1.2.1 2.23.140.1.2.2
5	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	51336A2AEFDB1F80EDB2C6D306D22593C4C8B666	2C154235528D701790B675AFF6E1970827B10ED665E913835BF46E3460FD5C84	-
6	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	-
7	1	CN = SECOM Passport for Web SR 3.0 CA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B12F4D05F9ED13	rsaEncryption	2048bit	sha256WithRSAEncryption	Mar 16 05:49:12 2018 GMT	Mar 16 05:49:12 2028 GMT	CBEF3DEF8374A1A842F03B4036FA6D8294A92736	E05ED4A9E4C773308A93E849861225AE349A92BBD4BACDD4900AD4E73B131100	2.23.140.1.2.2



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	ダイジェスタアルゴリズム	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	ポリシーオブジェクト識別子
8	1	CN = NII Open Domain CA - G7 RSA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18587A69943B5EC368F4CAF68F7	rsaEncryption	2048bit	sha256WithRSAEncryption	Dec 15 08:46:22 2020 GMT	May 29 05:00:39 2029 GMT	B02EE551EDFC4ACFA387F11390762D9D8E94A1E3	603DB707A584003BED6F1D43DCD4EAE13CD18D798E827DE2F3A31F3193FC0DAC	2.23.140.1.2.2
9	1	CN=NII Open Domain CA - G7 ECC O=SECOM Trust Systems CO.,LTD. C=JP	CN=Security Communication ECC RootCA1 O=SECOM Trust Systems CO.,LTD. C=JP	0100004C9F5DEB113CD4FB41C8C9EC7D	ECDSAEncryption	384bit	sha384WithECDSAEncryption	Dec 15 09:17:38 2020 GMT	Dec 15 09:17:38 2030 GMT	6B30200CAEB7C3139BD9A759178A5E30C14C5549	81CD03067252FFE849B240DCC24566678677E3F5FEDC4C540D7A26CAD2C081C8	2.23.140.1.2.2
10	1	CN = CrossTrust OV CA5 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B152643B58B011	rsaEncryption	2048bit	sha256WithRSAEncryption	Aug 22 07:23:58 2018 GMT	Aug 22 07:23:58 2028 GMT	24B7B441D4324FC419FF5E62643B5E69276117DC	79C4091B05B15C1683128B7A355E0AAD62E1BBBC3E5F3735370C06CC4D1AFB44	2.23.140.1.2.2
11	1	CN = SECOM Passport for Web EV 2.0 CA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B0C9	rsaEncryption	2048bit	sha256WithRSAEncryption	Dec 16 07:04:09 2014 GMT	Dec 16 07:04:09 2024 GMT	164BFB0C97388A185A54A146CF892447CCC476B3	E1F2E95000F815E11C81490430B5D02C8D81D0D256C85DF68B516D6C27761926	2.23.140.1.1



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	ダイジェスタアルゴリズム	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	ポリシーオブジェクト識別子
11	2	CN = SECOM Passport for Web EV 2.0 CA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B19D60F2 A361D7FA7E95 7C63BD5C	rsaEncryption	2048bit	sha256With RSAEncryption	Aug 30 04:35:47 2023 GMT	May 29 05:00:39 2029 GMT	164BFB0C97388A 185A54A146CF89 2447CCC476B3	39B6E3B388F749521DF2B354182EB4CD87D4BF36439BFAF0202E5596CFC2CAA4	2.23.140.1.1
12	1	CN = SECOM Passport for CodeSigning CA G2 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100004ECD64 452CBAA77EE 74E33D048	rsaEncryption	4096bit	sha384With RSAEncryption	May 25 01:37:39 2021 GMT	May 25 01:37:39 2031 GMT	4C6C10EB253A48 93C35BBE3DB68 CFB9EFDB64A65	BB974448A25466F597A55772577FD6C69FDC4D9F8D2B2D8A0232D04E77D52C8C	2.23.140.1.4.1
12	2	CN = SECOM Passport for CodeSigning CA G2 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B180E465 8AB862062FC7 602DB247	rsaEncryption	4096bit	sha256With RSAEncryption	Aug 6 08:53:55 2020 GMT	May 29 05:00:39 2029 GMT	4C6C10EB253A48 93C35BBE3DB68 CFB9EFDB64A65	2A2AC8DE79A38177699A34FA06D3E5FB86C27CDD0CAF3B332C8D861D0A753639	2.23.140.1.4.1
13	1	CN = SECOM Passport for Member PUB CA4 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B15750754 87009	rsaEncryption	2048bit	sha256With RSAEncryption	Oct 4 05:28:09 2018 GMT	Oct 4 05:28:09 2028 GMT	488C6576D21EAB F5FF3824B6C436 D90A9FA0BCAE	B10861737B3EC9B11FA6154D23970FFB2DABFC28AE6A6BF56C3F3204266239AD	-



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	ダイジェスタアルゴリズム	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	ポリシーオブジェクト識別子
13	2	CN = SECOM Passport for Member PUB CA4 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B0BC	rsaEncryption	2048bit	sha256With RSAEncryption	Nov 20 02:18:46 2013 GMT	Nov 20 02:18:46 2023 GMT	488C6576D21EAB F5FF3824B6C436 D90A9FA0BCAE	0940451DFECB675B5204C8AE07189D4E4E90957CFD2BAFDCFF36DB20C279E91A	-
14	1	CN = SECOM Passport for Member PUB CA5 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B16DA7E6 F3BBBA	rsaEncryption	2048bit	sha256With RSAEncryption	May 20 07:10:35 2020 GMT	May 29 05:00:39 2029 GMT	8939416491E946A 4165907F22BAF5 27F7D4BDA92	8C6DB8171AE6785F05426AE58C3D36F7559352202E9209B9D29B1BD447961DC8	-
14	2	CN = SECOM Passport for Member PUB CA5 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B0E1D249 6D57C4	rsaEncryption	2048bit	sha256With RSAEncryption	Aug 12 04:48:29 2015 GMT	Aug 12 04:48:29 2025 GMT	8939416491E946A 4165907F22BAF5 27F7D4BDA92	C931A0F85A052901234A54FD460D417F1A8B63C38C4811F79B98F3AE1C2FE9FB	-
15	1	CN = SECOM Passport for Member PUB CA8 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B12B288A 041897	rsaEncryption	2048bit	sha256With RSAEncryption	Jan 9 06:01:29 2018 GMT	Jan 9 06:01:29 2028 GMT	762BD98DCC353 6324505DF9E8C6 A17D133DC0307	7A4FCBA079F5BDDCF0A76C3B03A377E155A53009474A1B3EB8F34961A53BDA9C	-



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	ダイジェスタアルゴリズム	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	ポリシーオブジェクト識別子
16	1	CN = SECOM Passport for PublicID SMIME RSA CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B19AF338 0D8F037998731 AA1D930	rsaEncryption	4096bit	sha384With RSAEncryption	Jun 7 04:33:22 2023 GMT	May 29 05:00:39 2029 GMT	0136A8AB68C0C 698FA996CC6A4F A92A83714E2D2	DB088F140ACBE85FA1EC83D3851063803FFD8471564CF852B92A60FEB965A02F	2.23.140.1.5.1.3
17	1	CN = SECOM Passport for Member PUB CA7 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18CA759 8FE1D7178D01 69AC380F	rsaEncryption	2048bit	sha256With RSAEncryption	Jul 12 06:32:24 2021 GMT	May 29 05:00:39 2029 GMT	BD085E25849CF D3524D81DC7306 C789DC1A4BB20	BA08827159A8510FDF274383DCC44E70423416DF862B972F8945AAF49E30D5A4	-
18	1	CN = SECOM Passport for PublicID Document Signing RSA CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	010000041C223 AF622A83408E B6D397D	rsaEncryption	4096bit	sha384With RSAEncryption	Feb 24 06:53:38 2023 GMT	Feb 1 00:00:00 2043 GMT	B72166C25545E7 934EA2C8AD5DB 4063242CEE1D9	368A62B89C9713662E409AB7DF722525D6B226551B518F960559EE1DF0FFA16E	-
19	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	rsaEncryption	4096bit	sha384With RSAEncryption	Feb 24 07:41:36 2023 GMT	Feb 1 00:00:00 2043 GMT	8939416491E946A 4165907F22BAF5 27F7D4BDA92	D2A60B7C6DFE267AD055DA26BF68D9F1478D862310F3DD0A73325941C2F00DDE	-



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	ダイジェスタアルゴリズム	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	ポリシーオブジェクト識別子
20	1	CN = SMBC Certificate Authority CA2 OU = SMBC Authority O = Sumitomo Mitsui Banking Corporation C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18FB4B469F41224BD4D771CD48F	rsaEncryption	2048bit	sha256WithRSAEncryption	Aug 13 05:45:33 2021 GMT	May 29 05:00:39 2029 GMT	5F2B8D9DBA6B0CADE15F17616448A0952A96F087	7B2EE6E46480EE7C43F759D45BEDBD3D7A5BEDEE8B888CEAAB3D811644AC4682	
21	1	CN = SMBC Certificate Authority CA2 G2 OU = SMBC Authority O = Sumitomo Mitsui Banking Corporation C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100004AF02424DAF397BD4AEA6B8D10	rsaEncryption	2048bit	sha384WithRSAEncryption	Nov 6 05:09:15 2020 GMT	Dec 31 14:59:59 2030 GMT	0DA7566D6FE3CEA31BAADB0252F7109D314442FF	FB6F8CF1EB756CB6C1E61571CADADC46FFA8871F686CAA0F775B25A8B8AD701	
22	1	CN = SECOM TimeStamping CA3 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100003E344C91C7CC	rsaEncryption	4096bit	sha384WithRSAEncryption	Jun 7 05:12:31 2018 GMT	Dec 31 05:12:31 2037 GMT	199DFABC5C3455AF3CC59B4DBBA3A59639288844	0E984339724A267C2A3DC4FCC8D020B3B4BA329A0AD7E390CFBF76E88823E11B	
23	1	CN = SECOM TimeStamping CA4 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100004BD4F49CF31A08CB1F6953D0DD	rsaEncryption	4096bit	sha384WithRSAEncryption	Dec 15 09:48:40 2020 GMT	Dec 31 14:59:59 2037 GMT	60811F0DE823DC6EB01949BEE7F90D2448C19DB6	3CFC266D4E23BCF70E99CC7918ED578A300498F00C8BBD123250BDEE5A2BEC5B	2.23.140.1.4.2



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	ダイジェスタアルゴリズム	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	ポリシーオブジェクト識別子
23	2	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	60811F0DE823DC6EB01949BEE7F90D2448C19DB6	9B7A75CCF8D0EDAC6088D40F14B6D20C85C69B2B7F5A2C957FB1C2BC5870BAF5	
24	1	CN = SECOM TimeStamping CA2 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18D4E99D73CB4EC2BEA646E1AE6	rsaEncryption	2048bit	sha256WithRSAEncryption	Jul 12 06:47:19 2021 GMT	May 29 05:00:39 2029 GMT	074D137DEAB7FAED93D493773F581300CBE12389	2AF80BCD3A5A53406FF22271DB84B938417E8C338E5AA28CC47575FD41F22615	
25	1	CN = CrossTrust DV CA5 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B15323E5AEFDCCD	rsaEncryption	2048bit	sha256WithRSAEncryption	Aug 22 07:32:24 2018 GMT	Aug 22 07:32:24 2028 GMT	4F8B70CFA9401C96E5945D77ACD66F4D2D9BF277	18F4368FE93B3CAE025230BCE7EAD340FD90FB27F9A10E36FEE89FC454F22788	2.23.140.1.2.1
26	1	CN = FujiSSL Public Validation Authority - G3 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B154F33C5E5E00	rsaEncryption	2048bit	sha256WithRSAEncryption	Aug 22 07:41:02 2018 GMT	Aug 22 07:41:02 2028 GMT	BCEBD911E051646FFFF0744F0D5AAB4A4F2D7827	56DA6EFEF1D504134C72EEDC3AE44AA7FA11B848820DBFAA86CA8E35D60EDB04	2.23.140.1.2.1



付録 B

証明書ポリシー

CA	CP名	Version	日付
CA#1 CA#2	Security Communication RootCA 下位 CA 用証明書ポリシー	6.05	2024/4/1
CA#3 CA#4	Security Communication RootCA 下位 CA 用証明書ポリシー	6.04	2024/1/24
CA#5 CA#6	Security Communication RootCA 下位 CA 用証明書ポリシー	6.03	2023/7/11
	Security Communication RootCA 下位 CA 用証明書ポリシー	6.02	2023/5/17
CA#1 CA#2 CA#3	Security Communication RootCA タイムスタンプサービス用証明書ポリシー	5.09	2024/1/24
CA#4 CA#5 CA#6	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#7	セコムパスポート for Web SR 認証局証明書ポリシー	3.04	2024/4/1
	セコムパスポート for Web SR 認証局証明書ポリシー	3.03	2023/8/28
	セコムパスポート for Web SR 認証局証明書ポリシー	3.02	2023/5/17
CA#8	企業認証 証明書ポリシー	1.22	2024/4/1
CA#9	企業認証 証明書ポリシー	1.21	2023/8/28
CA#10	企業認証 証明書ポリシー	1.20	2023/5/17
CA#11	セコムパスポート for Web EV 認証局証明書ポリシー	3.04	2024/4/1
	セコムパスポート for Web EV 認証局証明書ポリシー	3.03	2023/9/14
	セコムパスポート for Web EV 認証局証明書ポリシー	3.02	2023/8/28
	セコムパスポート for Web EV 認証局証明書ポリシー	3.01	2023/5/17
CA#12 CA#13	セコムパスポート for Member 2.0 PUB 証明書ポリシー	6.07	2024/5/17
CA#14 CA#15	セコムパスポート for Member 2.0 PUB 証明書ポリシー	6.06	2024/4/1
CA#16 CA#17	セコムパスポート for Member 2.0 PUB 証明書ポリシー	6.05	2023/8/28
CA#18 CA#19	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
CA#20 CA#21	三井住友銀行の電子契約サービス 証明書ポリシー／認証局運用規定	1.5	2023/5/1
CA#22	SECOM TimeStamping CA タイムスタンプサービス用証明書ポリシー	5.07	2024/7/12
CA#23	SECOM TimeStamping CA タイムスタンプサービス用証明書ポリシー	5.06	2024/4/1
CA#24	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
CA#25	ドメイン認証 証明書ポリシー	1.22	2024/4/1
CA#26	ドメイン認証 証明書ポリシー	1.21	2023/8/28
	ドメイン認証 証明書ポリシー	1.20	2023/5/17



運用規程

CA	CPS 名	Version	日付
CA#1	Security Communication RootCA 認証運用規定	6.04	2024/4/1
CA#2			
CA#3	Security Communication RootCA 認証運用規定	6.03	2024/1/24
CA#4			
CA#5	Security Communication RootCA 認証運用規定	6.02	2023/5/17
CA#6			
CA#7	セコム電子認証基盤認証運用規程	2.19	2024/4/1
CA#8			
CA#9			
CA#10			
CA#11			
CA#12			
CA#13			
CA#14			
CA#15			
CA#16	セコム電子認証基盤認証運用規程	2.18	2023/5/17
CA#17			
CA#18			
CA#19			
CA#22			
CA#23			
CA#24			
CA#25			
CA#26			
CA#20	三井住友銀行の電子契約サービス 証明書ポリシー／認証局運用規定	1.5	2023/5/1
CA#21			



付録 C

#	開示内容	公開リンク
1	SECOM: Certificates Issued with lower case value in subject:countryName	https://bugzilla.mozilla.org/show_bug.cgi?id=1896596
2	SECOM: Difference in upper and lower case between CN field and SAN	https://bugzilla.mozilla.org/show_bug.cgi?id=1897346

経営者の記述書

2024年8月26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

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6月7日から2024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 ビジネス実務の管理

- ・ 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 ブラウザフォーラムを構成するインターネットブラウザのオンラインフォーラムである Bugzilla のサイトで公開されている情報を[付録 C](#)に記載している。

付録 A の「対象 CA の識別情報」に記載されている CA #1-1 は、2023 年 9 月 30 日に廃止した。

CA #13-2 は、2023 年 11 月 20 日に廃止した。

CA #23-2 は、2023 年 11 月 11 日から 2023 年 11 月 16 日までの期間において、証明書を発行せず、失効ステータス情報のみをオンラインで提供していた。また、2023 年 11 月 16 日に廃止した。

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: Security Communication RootCA1
CA#2: Security Communication RootCA2
CA#3: Security Communication RootCA3
CA#4: Security Communication ECCRootCA1
CA#5: SECOM RSA Root CA 2023
CA#6: SECOM Document Signing RSA Root CA 2023
OV SSL Issuing CAs
CA#7: SECOM Passport for Web SR 3.0 CA
CA#8: NII Open Domain CA - G7 RSA
CA#9: NII Open Domain CA - G7 ECC
CA#10: CrossTrust OV CA5
EV SSL Issuing CAs
CA#11: SECOM Passport for Web EV 2.0 CA
Non-EV Code Signing Issuing CAs
CA#12: SECOM Passport for CodeSigning CA G2
Secure Email (S/MIME) CAs
CA#13: SECOM Passport for Member PUB CA4
CA#14: SECOM Passport for Member PUB CA5
CA#15: SECOM Passport for Member PUB CA8
CA#16: SECOM Passport for PublicID SMIME RSA CA 2023

Document Signing CAs
CA#17: SECOM Passport for Member PUB CA7
CA#18: SECOM Passport for PublicID Document Signing RSA CA 2023
CA#19: SECOM Passport for PublicID AATL RSA CA 2023
CA#20: SMBC Certificate Authority CA2
CA#21: SMBC Certificate Authority CA2 G2
Timestamp CAs
CA#22: SECOM TimeStamping CA3
CA#23: SECOM TimeStamping CA4
CA#24: SECOM TimeStamping CA2
Other CAs
CA#25: CrossTrust DV CA5
CA#26: FujiSSL Public Validation Authority - G3

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	ポリシーオブジェクト識別子
1	1	OU = Security Communication RootCA1 O = SECOM Trust.net C = JP	OU = Security Communication RootCA1 O = SECOM Trust.net C = JP	00	rsaEncryption	2048bit	sha1WithRSAEncryption	Sep 30 04:20:49 2003 GMT	Sep 30 04:20:49 2023 GMT	A073499968DC855B65E39B282F579FBD33BC0748	E75E72ED9F560EEC6EB4800073A43FC3AD19195A392282017895974A99026B6C	-
2	1	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	00	rsaEncryption	2048bit	sha256WithRSAEncryption	May 29 05:00:39 2009 GMT	May 29 05:00:39 2029 GMT	0A85A9776505987C4081F80F972C38F10AEC3CCF	513B2CECB810D4CDE5DD85391ADFC6C2DD60D87BB736D2B521484AA47A0EBEF6	2.23.140.1.2.1 2.23.140.1.2.2 2.23.140.1.1 2.23.140.1.4.1 2.23.140.1.5.1.3
3	1	OU = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	00E17C3740FD1BFE67	rsaEncryption	4096bit	sha384WithRSAEncryption	Jun 16 06:17:16 2016 GMT	Jan 18 06:17:16 2038 GMT	64147CFC587216A60A2934156F2ACBBCFCFAFA8AB	24A55C2AB051442D0617766541239A4AD032D7C55175AA34FFDE2FBC4F5C5294	2.23.140.1.4.1 2.23.140.1.4.2
4	1	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	00D65D9BB378812EEB	ECDSAEncryption	384bit	sha384WithECDSAEncryption	Jun 16 05:15:28 2016 GMT	Jan 18 05:15:28 2038 GMT	861CE7FE2DA54A8B08FE2811FABEA366F860592F	E74FBDA55BD564C473A36B441AA799C8A68E077440E8288B9FA1E50E4BBACA11	2.23.140.1.2.1 2.23.140.1.2.2
4	2	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B1A49DB1D47C2674294CEE84F8FC	ECDSAEncryption	384bit	sha384WithECDSAEncryption	Apr 4 06:22:18 2024 GMT	May 29 05:00:39 2029 GMT	861CE7FE2DA54A8B08FE2811FABEA366F860592F	C3EBCEA7E6B13AC3EB3A79F05819E67D6893C65642F50D9B5E1647CB26506B8E	2.23.140.1.2.1 2.23.140.1.2.2

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	ポリシーオブジェクト識別子
5	I	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	51336A2AEFDB1F80EDB2C6D306D22593C4C8B666	2C154235528D701790B675AFF6E1970827B10ED665E913835BF46E3460FD5C84	-
6	I	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	-
7	I	CN = SECOM Passport for Web SR 3.0 CA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B12F4D05F9ED13	rsaEncryption	2048bit	sha256WithRSAEncryption	Mar 16 05:49:12 2018 GMT	Mar 16 05:49:12 2028 GMT	CBEF3DEF8374A1A842F03B4036FA6D8294A92736	E05ED4A9E4C773308A93E849861225AE349A92BBD4BACDD4900AD4E73B131100	2.23.140.1.2.2
8	I	CN = NII Open Domain CA - G7 RSA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18587A69943B5EC368F4CAF68F7	rsaEncryption	2048bit	sha256WithRSAEncryption	Dec 15 08:46:22 2020 GMT	May 29 05:00:39 2029 GMT	B02EE551EDFC4ACFA387F11390762D9D8E94A1E3	603DB707A584003BED6F1D43DCD4EAE13CD18D798E827DE2F3A31F3193FC0DAC	2.23.140.1.2.2
9	I	CN=NII Open Domain CA - G7 ECC O=SECOM Trust Systems CO.,LTD. C=JP	CN=Security Communication ECC RootCA1 O=SECOM Trust Systems CO.,LTD. C=JP	0100004C9F5DEB113CD4FB41C8C9EC7D	ECDSAEncryption	384bit	sha384WithECDSAEncryption	Dec 15 09:17:38 2020 GMT	Dec 15 09:17:38 2030 GMT	6B30200CAEB7C3139BD9A759178A5E30C14C5549	81CD03067252FFE849B240DCC24566678677E3F5FEDC4C540D7A26CAD2C081C8	2.23.140.1.2.2

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	ディジタル署名アルゴリズム	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	ポリシーオブジェクト識別子
10	1	CN = CrossTrust OV CA5 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B152643B58B011	rsaEncryption	2048bit	sha256WithRSAEncryption	Aug 22 07:23:58 2018 GMT	Aug 22 07:23:58 2028 GMT	24B7B441D4324FC419FF5E62643B5E69276117DC	79C4091B05B15C1683128B7A355E0AAD62E1BBBC3E5F3735370C06CC4D1AFB44	2.23.140.1.2.2
11	1	CN = SECOM Passport for Web EV 2.0 CA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B0C9	rsaEncryption	2048bit	sha256WithRSAEncryption	Dec 16 07:04:09 2014 GMT	Dec 16 07:04:09 2024 GMT	164BFB0C97388A185A54A146CF892447CCC476B3	E1F2E95000F815E11C81490430B5D02C8D81D0D256C85DF68B516D6C27761926	2.23.140.1.1
11	2	CN = SECOM Passport for Web EV 2.0 CA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B19D60F2A361D7FA7E957C63BD5C	rsaEncryption	2048bit	sha256WithRSAEncryption	Aug 30 04:35:47 2023 GMT	May 29 05:00:39 2029 GMT	164BFB0C97388A185A54A146CF892447CCC476B3	39B6E3B388F749521DF2B354182EB4CD87D4BF36439BFAF020E5596CFC2CAA4	2.23.140.1.1
12	1	CN = SECOM Passport for CodeSigning CA G2 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100004ECD64452CBAA77EE74E33D048	rsaEncryption	4096bit	sha384WithRSAEncryption	May 25 01:37:39 2021 GMT	May 25 01:37:39 2031 GMT	4C6C10EB253A4893C35BBE3DB68CFB9EFDB64A65	BB974448A25466F597A55772577FD6C69FDC4D9F8D2B2D8A0232D04E77D52C8C	2.23.140.1.4.1
12	2	CN = SECOM Passport for CodeSigning CA G2 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B180E4658AB862062FC7602DB247	rsaEncryption	4096bit	sha256WithRSAEncryption	Aug 6 08:53:55 2020 GMT	May 29 05:00:39 2029 GMT	4C6C10EB253A4893C35BBE3DB68CFB9EFDB64A65	2A2AC8DE79A38177699A34FA06D3E5FB86C27CDD0CAF3B332C8D861D0A753639	2.23.140.1.4.1

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	ディジタル署名	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	ポリシーオブジェクト識別子
13	1	CN = SECOM Passport for Member PUB CA4 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B15750754 87009	rsaEncryption	2048bit	sha256With RSAEncryption	Oct 4 05:28:09 2018 GMT	Oct 4 05:28:09 2028 GMT	488C6576D21EAB F5FF3824B6C436 D90A9FA0BCAE	B10861737B3EC9B11FA6154D23970FFB2DABFC28AE6A6BF56C3F3204266239AD	-
13	2	CN = SECOM Passport for Member PUB CA4 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B0BC	rsaEncryption	2048bit	sha256With RSAEncryption	Nov 20 02:18:46 2013 GMT	Nov 20 02:18:46 2023 GMT	488C6576D21EAB F5FF3824B6C436 D90A9FA0BCAE	0940451DFECB675B5204C8AE07189D4E4E90957CFD2BAFDCFF36DB20C279E91A	-
14	1	CN = SECOM Passport for Member PUB CA5 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B16DA7E6 F3BBBA	rsaEncryption	2048bit	sha256With RSAEncryption	May 20 07:10:35 2020 GMT	May 29 05:00:39 2029 GMT	8939416491E946A 4165907F22BAF5 27F7D4BDA92	8C6DB8171AE6785F05426AE58C3D36F755935220E9209B9D29B1BD447961DC8	-
14	2	CN = SECOM Passport for Member PUB CA5 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B0E1D249 6D57C4	rsaEncryption	2048bit	sha256With RSAEncryption	Aug 12 04:48:29 2015 GMT	Aug 12 04:48:29 2025 GMT	8939416491E946A 4165907F22BAF5 27F7D4BDA92	C931A0F85A052901234A54FD460D417F1A8B63C38C4811F79B98F3AE1C2FE9FB	-

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	ダイジェスタアルゴリズム	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	ポリシーオブジェクト識別子
15	I	CN = SECOM Passport for Member PUB CA8 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B12B288A 041897	rsaEncryption	2048bit	sha256With RSAEncryption	Jan 9 06:01:29 2018 GMT	Jan 9 06:01:29 2028 GMT	762BD98DCC353 6324505DF9E8C6 A17D133DC0307	7A4FCBA079F5BDDCF0A76C3B03A377E155A53009474A1B3EB8F34961A53BDA9C	-
16	I	CN = SECOM Passport for PublicID SMIME RSA CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B19AF338 0D8F037998731 AA1D930	rsaEncryption	4096bit	sha384With RSAEncryption	Jun 7 04:33:22 2023 GMT	May 29 05:00:39 2029 GMT	0136A8AB68C0C 698FA996CC6A4F A92A83714E2D2	DB088F140ACBE85FA1EC83D3851063803FFD8471564CF852B92A60FEB965A02F	2.23.140.1.5.1.3
17	I	CN = SECOM Passport for Member PUB CA7 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18CA759 8FE1D7178D01 69AC380F	rsaEncryption	2048bit	sha256With RSAEncryption	Jul 12 06:32:24 2021 GMT	May 29 05:00:39 2029 GMT	BD085E25849CF D3524D81DC7306 C789DC1A4BB20	BA08827159A8510FDF274383DCC44E70423416DF862B972F8945AAF49E30D5A4	-
18	I	CN = SECOM Passport for PublicID Document Signing RSA CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	010000041C223 AF622A83408E B6D397D	rsaEncryption	4096bit	sha384With RSAEncryption	Feb 24 06:53:38 2023 GMT	Feb 1 00:00:00 2043 GMT	B72166C25545E7 934EA2C8AD5DB 4063242CEE1D9	368A62B89C9713662E409AB7DF722525D6B226551B518F960559EE1DF0FFA16E	-

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	ポリシーオブジェクト識別子
19	I	CN = SECOM Passport for PublicID AATL RSA CA 2023 O = SECOM Trust 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	rsaEncryption	4096bit	sha384With RSAEncryption	Feb 24 07:41:36 2023 GMT	Feb 1 00:00:00 2043 GMT	8939416491E946A 4165907F22BAF5 27F7D4BDA92	D2A60B7C6DFE267AD055DA26BF68D9F1478D862310F3DD0A73325941C2F00DDE	-
20	I	CN = SMBC Certificate Authority CA2 OU = SMBC Authority O = Sumitomo Mitsui Banking Corporation C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18FB4B4 69F41224BD4D 771CD48F	rsaEncryption	2048bit	sha256With RSAEncryption	Aug 13 05:45:33 2021 GMT	May 29 05:00:39 2029 GMT	5F2B8D9DBA6B0 CADE15F1761644 8A0952A96F087	7B2EE6E46480EE7C43F759D45BEDBD3D7A5BEDEE8B888CEAAB3D811644AC4682	-
21	I	CN = SMBC Certificate Authority CA2 G2 OU = SMBC Authority O = Sumitomo Mitsui Banking Corporation C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100004AF0242 4DAF397BD4A EA6B8D10	rsaEncryption	2048bit	sha384With RSAEncryption	Nov 6 05:09:15 2020 GMT	Dec 31 14:59:59 2030 GMT	0DA7566D6FE3C EA31BAADB0252 F7109D314442FF	FB6F8CF1EB756CB6C1E61571CADADC46FFA8871F686CAA0F775B25A8B8AD701	-
22	I	CN = SECOM TimeStamping CA3 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100003E344C9 1C7CC	rsaEncryption	4096bit	sha384With RSAEncryption	Jun 7 05:12:31 2018 GMT	Dec 31 05:12:31 2037 GMT	199DFABC5C345 5AF3CC59B4DBB A3A59639288844	0E984339724A267C2A3DC4FCC8D020B3B4BA329A0AD7E390CFBF76E88823E11B	-

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	ディジタル署名	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	ポリシーオブジェクト識別子
23	1	CN = SECOM TimeStamping CA4 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100004BD4F49CF31A08CB1F6953D0DD	rsaEncryption	4096bit	sha384WithRSAEncryption	Dec 15 09:48:40 2020 GMT	Dec 31 14:59:59 2037 GMT	60811F0DE823DC6EB01949BEE7F90D2448C19DB6	3CFC266D4E23BCF70E99CC7918ED578A300498F00C8BBD123250BDEE5A2BEC5B	2.23.140.1.4.2
23	2	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	60811F0DE823DC6EB01949BEE7F90D2448C19DB6	9B7A75CCF8D0EDAC6088D40F14B6D20C85C69B2B7F5A2C957FB1C2BC5870BAF5	-
24	1	CN = SECOM TimeStamping CA2 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18D4E99D73CB4EC2BEA646E1AE6	rsaEncryption	2048bit	sha256WithRSAEncryption	Jul 12 06:47:19 2021 GMT	May 29 05:00:39 2029 GMT	074D137DEAB7FAED93D493773F581300CBE12389	2AF80BCD3A5A53406FF22271DB84B938417E8C338E5AA28CC47575FD41F22615	-
25	1	CN = CrossTrust DV CA5 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B15323E5AEFDCD	rsaEncryption	2048bit	sha256WithRSAEncryption	Aug 22 07:32:24 2018 GMT	Aug 22 07:32:24 2028 GMT	4F8B70CFA9401C96E5945D77ACD66F4D2D9BF277	18F4368FE93B3CAE025230BCE7EAD340FD90FB27F9A10E36FEE89FC454F22788	2.23.140.1.2.1
26	1	CN = FujiSSL Public Validation Authority - G3 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B154F33C5E5E00	rsaEncryption	2048bit	sha256WithRSAEncryption	Aug 22 07:41:02 2018 GMT	Aug 22 07:41:02 2028 GMT	BCEBD911E051646FFF0744F0D5AAB4A4F2D7827	56DA6EFEF1D504134C72EEDC3AE44AA7FA11B848820DBFAA86CA8E35D60EDB04	2.23.140.1.2.1

付録 B

証明書ポリシー

CA	CP 名	Version	日付
CA#1 CA#2	Security Communication RootCA 下位 CA 用証明書ポリシー	6.05	2024/4/1
CA#3 CA#4	Security Communication RootCA 下位 CA 用証明書ポリシー	6.04	2024/1/24
CA#5 CA#6	Security Communication RootCA 下位 CA 用証明書ポリシー	6.03	2023/7/11
	Security Communication RootCA 下位 CA 用証明書ポリシー	6.02	2023/5/17
CA#1 CA#2 CA#3	Security Communication RootCA タイムスタンプサービス用証明書ポリシー	5.09	2024/1/24
CA#4 CA#5 CA#6	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#7	セコムパスポート for Web SR 認証局証明書ポリシー	3.04	2024/4/1
	セコムパスポート for Web SR 認証局証明書ポリシー	3.03	2023/8/28
	セコムパスポート for Web SR 認証局証明書ポリシー	3.02	2023/5/17
CA#8	企業認証 証明書ポリシー	1.22	2024/4/1
CA#9	企業認証 証明書ポリシー	1.21	2023/8/28
CA#10	企業認証 証明書ポリシー	1.20	2023/5/17
CA#11	セコムパスポート for Web EV 認証局証明書ポリシー	3.04	2024/4/1
	セコムパスポート for Web EV 認証局証明書ポリシー	3.03	2023/9/14
	セコムパスポート for Web EV 認証局証明書ポリシー	3.02	2023/8/28
	セコムパスポート for Web EV 認証局証明書ポリシー	3.01	2023/5/17
CA#12 CA#13	セコムパスポート for Member 2.0 PUB 証明書ポリシー	6.07	2024/5/17
CA#14 CA#15	セコムパスポート for Member 2.0 PUB 証明書ポリシー	6.06	2024/4/1
CA#16 CA#17	セコムパスポート for Member 2.0 PUB 証明書ポリシー	6.05	2023/8/28
CA#18 CA#19	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
CA#20 CA#21	三井住友銀行の電子契約サービス 証明書ポリシー／認証局運用規定	1.5	2023/5/1
CA#22	SECOM TimeStamping CA タイムスタンプサービス用証明書ポリシー	5.07	2024/7/12
CA#23	SECOM TimeStamping CA タイムスタンプサービス用証明書ポリシー	5.06	2024/4/1
CA#24	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

CA	CP 名	Version	日付
CA#25	ドメイン認証 証明書ポリシー	1.22	2024/4/1
CA#26	ドメイン認証 証明書ポリシー	1.21	2023/8/28
	ドメイン認証 証明書ポリシー	1.20	2023/5/17

運用規程

CA	CPS 名	Version	日付
CA#1	Security Communication RootCA 認証運用規定	6.04	2024/4/1
CA#2			
CA#3	Security Communication RootCA 認証運用規定	6.03	2024/1/24
CA#4			
CA#5	Security Communication RootCA 認証運用規定	6.02	2023/5/17
CA#6			
CA#7	セコム電子認証基盤認証運用規程	2.19	2024/4/1
CA#8			
CA#9			
CA#10			
CA#11			
CA#12			
CA#13			
CA#14			
CA#15			
CA#16	セコム電子認証基盤認証運用規程	2.18	2023/5/17
CA#17			
CA#18			
CA#19			
CA#22			
CA#23			
CA#24			
CA#25			
CA#26			
CA#20	三井住友銀行の電子契約サービス 証明書ポリシー／認証局運用規定	1.5	2023/5/1
CA#21			

付録 C

#	開示内容	公開リンク
1	SECOM: Certificates Issued with lower case value in subject:countryName	https://bugzilla.mozilla.org/show_bug.cgi?id=1896596
2	SECOM: Difference in upper and lower case between CN field and SAN	https://bugzilla.mozilla.org/show_bug.cgi?id=1897346

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 26, 2024

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 June 7, 2023 to June 6, 2024 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](#).

Appendix A, #1-1 CAs was revoked on September 30, 2023.

Appendix A, #13-2 CAs was revoked on November 20, 2023.

Appendix A, #23-2 CAs did not issue certificates during the period November 11, 2023 to November 16, 2023 and were maintained online to provide revocation status information only. Those CAs were also revoked on November 16, 2023.

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



(Translation)

(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.

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 June 7, 2023 to June 6, 2024, 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.

Other Matters

STS's management has disclosed to us the information enumerated in [Appendix C](#), that have been posted publicly on Bugzilla's site which is the online forums of individual internet browsers that comprise the CA/Browser Forum.

(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: Security Communication RootCA1
CA#2: Security Communication RootCA2
CA#3: Security Communication RootCA3
CA#4: Security Communication ECCRootCA1
CA#5: SECOM RSA Root CA 2023
CA#6: SECOM Document Signing RSA Root CA 2023
OV SSL Issuing CAs
CA#7: SECOM Passport for Web SR 3.0 CA
CA#8: NII Open Domain CA - G7 RSA
CA#9: NII Open Domain CA - G7 ECC
CA#10: CrossTrust OV CA5
EV SSL Issuing CAs
CA#11: SECOM Passport for Web EV 2.0 CA
Non-EV Code Signing Issuing CAs
CA#12: SECOM Passport for CodeSigning CA G2
Secure Email (S/MIME) CAs
CA#13: SECOM Passport for Member PUB CA4
CA#14: SECOM Passport for Member PUB CA5
CA#15: SECOM Passport for Member PUB CA8
CA#16: SECOM Passport for PublicID SMIME RSA CA 2023



(Translation)

Document Signing CAs
CA#17: SECOM Passport for Member PUB CA7
CA#18: SECOM Passport for PublicID Document Signing RSA CA 2023
CA#19: SECOM Passport for PublicID AATL RSA CA 2023
CA#20: SMBC Certificate Authority CA2
CA#21: SMBC Certificate Authority CA2 G2
Timestamp CAs
CA#22: SECOM TimeStamping CA3
CA#23: SECOM TimeStamping CA4
CA#24: SECOM TimeStamping CA2
Other CAs
CA#25: CrossTrust DV CA5
CA#26: FujiSSL Public Validation Authority - G3



(Translation)

CA Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
1	1	OU = Security Communication RootCA1 O = SECOM Trust.net C = JP	OU = Security Communication RootCA1 O = SECOM Trust.net C = JP	00	rsaEncryption	2048bit	sha1WithRSAEncryption	Sep 30 04:20:49 2003 GMT	Sep 30 04:20:49 2023 GMT	A073499968DC855B65E39B282F579FBD33BC0748	E75E72ED9F560EEC6EB4800073A43FC3AD19195A392282017895974A99026B6C	
2	1	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	00	rsaEncryption	2048bit	sha256WithRSAEncryption	May 29 05:00:39 2009 GMT	May 29 05:00:39 2029 GMT	0A85A9776505987C4081F80F972C38F10AEC3CCF	513B2CECB810D4CDE5DD85391ADFC6C2DD60D87BB736D2B521484AA47A0EBEF6	2.23.140.1.2.1 2.23.140.1.2.2 2.23.140.1.1 2.23.140.1.4.1 2.23.140.1.5.1.3
3	1	OU = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	00E17C3740FD1BFE67	rsaEncryption	4096bit	sha384WithRSAEncryption	Jun 16 06:17:16 2016 GMT	Jan 18 06:17:16 2038 GMT	64147CFC587216A60A2934156F2ACBBCFCAFA8AB	24A55C2AB051442D0617766541239A4AD032D7C55175AA34FFDE2FBC4F5C5294	2.23.140.1.4.1 2.23.140.1.4.2
4	1	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	00D65D9BB378812EEB	ECDSAEncryption	384bit	sha384WithECDSAEncryption	Jun 16 05:15:28 2016 GMT	Jan 18 05:15:28 2038 GMT	861CE7FE2DA54A8B08FE2811FABEA366F860592F	E74FBDA55BD564C473A36B441AA799C8A68E077440E8288B9FA1E50E4BBACA11	2.23.140.1.2.1 2.23.140.1.2.2
4	2	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B1A49DB1D47C2674294CEE84F8FC	ECDSAEncryption	384bit	sha384WithECDSAEncryption	Apr 4 06:22:18 2024 GMT	May 29 05:00:39 2029 GMT	861CE7FE2DA54A8B08FE2811FABEA366F860592F	C3EBCEA7E6B13AC3EB3A79F05819E67D6893C65642F50D9B5E1647CB26506B8E	2.23.140.1.2.1 2.23.140.1.2.2



(Translation)

Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
5	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	51336A2AEFDB1F80EDB2C6D306D22593C4C8B666	2C154235528D701790B675AFF6E1970827B10ED665E913835BF46E3460FD5C84	-
6	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	-
7	CN = SECOM Passport for Web SR 3.0 CA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B12F4D05F9ED13	rsaEncryption	2048bit	sha256WithRSAEncryption	Mar 16 05:49:12 2018 GMT	Mar 16 05:49:12 2028 GMT	CBEF3DEF8374A1A842F03B4036FA6D8294A92736	E05ED4A9E4C773308A93E849861225AE349A92BBD4BACDD4900AD4E73B131100	2.23.140.1.2.2
8	CN = NII Open Domain CA - G7 RSA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18587A69943B5EC368F4CAF68F7	rsaEncryption	2048bit	sha256WithRSAEncryption	Dec 15 08:46:22 2020 GMT	May 29 05:00:39 2029 GMT	B02EE551EDFC4ACFA387F11390762D9D8E94A1E3	603DB707A584003BED6F1D43DCD4EAE13CD18D798E827DE2F3A31F3193FC0DAC	2.23.140.1.2.2
9	CN=NII Open Domain CA - G7 ECC O=SECOM Trust Systems CO.,LTD. C=JP	CN=Security Communication ECC RootCA1 O=SECOM Trust Systems CO.,LTD. C=JP	0100004C9F5DEB113CD4FB41C8C9EC7D	ECDSEncryption	384bit	sha384WithECCSAEncryption	Dec 15 09:17:38 2020 GMT	Dec 15 09:17:38 2030 GMT	6B30200CAEB7C3139BD9A759178A5E30C14C5549	81CD03067252FFE849B240DCC24566678677E3F5FEDC4C540D7A26CAD2C081C8	2.23.140.1.2.2



(Translation)

Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
10	CN = CrossTrust OV CA5 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B152643B58B011	rsaEncryption	2048bit	sha256WithRSAEncryption	Aug 22 07:23:58 2018 GMT	Aug 22 07:23:58 2028 GMT	24B7B441D4324F79C419FF5E62643B5E69276117DC	79C4091B05B15C1683128B7A355E0AAD62E1BBBC3E5F3735370C06CC4D1AFB44	2.23.140.1.2.2
11	CN = SECOM Passport for Web EV 2.0 CA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B0C9	rsaEncryption	2048bit	sha256WithRSAEncryption	Dec 16 07:04:09 2014 GMT	Dec 16 07:04:09 2024 GMT	164BFB0C97388A185A54A146CF892447CCC476B3	E1F2E95000F815E11C81490430B5D02C8D81D0D256C85DF68B516D6C27761926	2.23.140.1.1
11	CN = SECOM Passport for Web EV 2.0 CA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B19D60F2A361D7FA7E957C63BD5C	rsaEncryption	2048bit	sha256WithRSAEncryption	Aug 30 04:35:47 2023 GMT	May 29 05:00:39 2029 GMT	164BFB0C97388A185A54A146CF892447CCC476B3	39B6E3B388F749521DF2B354182EB4CD87D4BF36439BFAF0202E5596CFC2CAA4	2.23.140.1.1
12	CN = SECOM Passport for CodeSigning CA G2 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100004ECD64452CBAA77EE74E33D048	rsaEncryption	4096bit	sha384WithRSAEncryption	May 25 01:37:39 2021 GMT	May 25 01:37:39 2031 GMT	4C6C10EB253A4893C35BBE3DB68CFB9EFDB64A65	BB974448A25466F597A55772577FD6C69FDC4D9F8D2B2D8A0232D04E77D52C8C	2.23.140.1.4.1
12	CN = SECOM Passport for CodeSigning CA G2 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B180E4658AB862062FC7602DB247	rsaEncryption	4096bit	sha256WithRSAEncryption	Aug 6 08:53:55 2020 GMT	May 29 05:00:39 2029 GMT	4C6C10EB253A4893C35BBE3DB68CFB9EFDB64A65	2A2AC8DE79A38177699A34FA06D3E5FB86C27CDD0CAF3B332C8D861D0A753639	2.23.140.1.4.1



(Translation)

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
13	1	CN = SECOM Passport for Member PUB CA4 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B1575075 487009	rsaEncr yption	2048bit	sha256With RSAEncryp tion	Oct 4 05:28:09 2018 GMT	Oct 4 05:28:09 2028 GMT	488C6576D21EA BF5FF3824B6C43 6D90A9FA0BCA E	B10861737B3EC9B11FA6154D23970FFB2DABFC28AE6A6BF56C3F3204266239AD	-
13	2	CN = SECOM Passport for Member PUB CA4 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B0BC	rsaEncr yption	2048bit	sha256With RSAEncryp tion	Nov 20 02:18:46 2013 GMT	Nov 20 02:18:46 2023 GMT	488C6576D21EA BF5FF3824B6C43 6D90A9FA0BCA E	0940451DFECB675B5204C8AE07189D4E4E90957CFD2BAFDCFF36DB20C279E91A	-
14	1	CN = SECOM Passport for Member PUB CA5 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B16DA7E 6F3BBBA	rsaEncr yption	2048bit	sha256With RSAEncryp tion	May 20 07:10:35 2020 GMT	May 29 05:00:39 2029 GMT	8939416491E946 A4165907F22BA F527F7D4BDA92	8C6DB8171AE6785F05426AE58C3D36F7559352202E9209B9D29B1BD447961DC8	-
14	2	CN = SECOM Passport for Member PUB CA5 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B0E1D249 6D57C4	rsaEncr yption	2048bit	sha256With RSAEncryp tion	Aug 12 04:48:29 2015 GMT	Aug 12 04:48:29 2025 GMT	8939416491E946 A4165907F22BA F527F7D4BDA92	C931A0F85A052901234A54FD460D417F1A8B63C38C4811F79B98F3AE1C2FE9FB	-



(Translation)

Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
15	1 CN = SECOM Passport for Member PUB CA8 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B12B288 A041897	rsaEncryption	2048bit	sha256With RSAEncryption	Jan 9 06:01:29 2018 GMT	Jan 9 06:01:29 2028 GMT	762BD98DCC353 6324505DF9E8C6 A17D133DC0307	7A4FCBA079F5BDDCF0A76C3B03A377E155A53009474A1B3EB8F34961A53BDA9C	-
16	1 CN = SECOM Passport for PublicID SMIME RSA CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B19AF338 0D8F03799873 1AA1D930	rsaEncryption	4096bit	sha384With RSAEncryption	Jun 7 04:33:22 2023 GMT	May 29 05:00:39 2029 GMT	0136A8AB68C0C 698FA996CC6A4 FA92A83714E2D 2	DB088F140ACBE85FA1EC83D3851063803FFD8471564CF852B92A60FEB965A02F	2.23.140.1.5.1.3
17	1 CN = SECOM Passport for Member PUB CA7 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18CA75 98FE1D7178D0 169AC380F	rsaEncryption	2048bit	sha256With RSAEncryption	Jul 12 06:32:24 2021 GMT	May 29 05:00:39 2029 GMT	BD085E25849CF D3524D81DC730 6C789DC1A4BB2 0	BA08827159A8510FDF274383DCC44E70423416DF862B972F8945AAF49E30D5A4	-
18	1 CN = SECOM Passport for PublicID Document Signing RSA CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	010000041C223 AF622A83408E B6D397D	rsaEncryption	4096bit	sha384With RSAEncryption	Feb 24 06:53:38 2023 GMT	Feb 1 00:00:00 2043 GMT	B72166C25545E7 934EA2C8AD5D B4063242CEE1D 9	368A62B89C9713662E409AB7DF722525D6B226551B518F960559EE1DF0FFA16E	-



(Translation)

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
19	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 RSAEncryp tion	Feb 24 07:41:36 2023 GMT	Feb 1 00:00:00 2043 GMT	8939416491E946 A4165907F22BA F527F7D4BDA92	D2A60B7C6DFE267AD055DA26BF68D9F1478D862310F3DD0A73325941C2F00DDE	-
20	1	CN = SMBC Certificate Authority CA2 OU = SMBC Authority O = Sumitomo Mitsui Banking Corporation C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18FB4B 469F41224BD4 D771CD48F	rsaEncr yption	2048bit	sha256With RSAEncryp tion	Aug 13 05:45:33 2021 GMT	May 29 05:00:39 2029 GMT	5F2B8D9DBA6B 0CADE15F17616 448A0952A96F08 7	7B2EE6E46480EE7C43F759D45BEDBD3D7A5BEDEE8B888CEAAB3D811644AC4682	-
21	1	CN = SMBC Certificate Authority CA2 G2 OU = SMBC Authority O = Sumitomo Mitsui Banking Corporation C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100004AF024 24DAF397BD4 AEA6B8D10	rsaEncr yption	2048bit	sha384With RSAEncryp tion	Nov 6 05:09:15 2020 GMT	Dec 31 14:59:59 2030 GMT	0DA7566D6FE3C EA31BAADB025 2F7109D314442F F	FB6F8CF1EB756CB6C1E61571CADADC46FFA8871F686CAAE0F775B25A8B8AD701	-
22	1	CN = SECOM TimeStamping CA3 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100003E344C 91C7CC	rsaEncr yption	4096bit	sha384With RSAEncryp tion	Jun 7 05:12:31 2018 GMT	Dec 31 05:12:31 2037 GMT	199DFABC5C345 5AF3CC59B4DB BA3A5963928884 4	0E984339724A267C2A3DC4FCC8D020B3B4BA329A0AD7E390CFBF76E88823E11B	-



(Translation)

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
23	1	CN = SECOM TimeStamping CA4 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100004BD4F49CF31A08CB1F6953D0DD	rsaEncryption	4096bit	sha384WithRSAEncryption	Dec 15 09:48:40 2020 GMT	Dec 31 14:59:59 2037 GMT	60811F0DE823DC6EB01949BEE7F90D2448C19DB6	3CFC266D4E23BCF70E99CC7918ED578A300498F00C8BBD123250BDEE5A2BEC5B	2.23.140.1.4.2
23	2	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	60811F0DE823DC6EB01949BEE7F90D2448C19DB6	9B7A75CCF8D0EDAC6088D40F14B6D20C85C69B2B7F5A2C957FB1C2BC5870BAF5	-
24	1	CN = SECOM TimeStamping CA2 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18D4E99D73CB4EC2BEA646E1AE6	rsaEncryption	2048bit	sha256WithRSAEncryption	Jul 12 06:47:19 2021 GMT	May 29 05:00:39 2029 GMT	074D137DEAB7F2AF80BCD3A5A53406FF22271DB84B938417E8C338E5AA28CC47575FD41F22615	2AF80BCD3A5A53406FF22271DB84B938417E8C338E5AA28CC47575FD41F22615	-
25	1	CN = CrossTrust DV CA5 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B15323E5AEFDCD	rsaEncryption	2048bit	sha256WithRSAEncryption	Aug 22 07:32:24 2018 GMT	Aug 22 07:32:24 2028 GMT	4F8B70CFA9401C96E5945D77ACD66F4D2D9BF277	18F4368FE93B3CAE025230BCE7EAD340FD90FB27F9A10E36FEE89FC454F22788	2.23.140.1.2.1
26	1	CN = FujiSSL Public Validation Authority - G3 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B154F33C5E5E00	rsaEncryption	2048bit	sha256WithRSAEncryption	Aug 22 07:41:02 2018 GMT	Aug 22 07:41:02 2028 GMT	BCEBD911E051646FFF0744F0D5AAB4A4F2D7827	56DA6EFEF1D504134C72EEDC3AE44A7FA11B848820DBFAA86CA8E35D60EDB04	2.23.140.1.2.1



(Translation)

APPENDIX B

Certificate Policy

CA	Policy Name	Version	Date
CA#1 CA#2	Security Communication RootCA Subordinate CA Certificate Policy	6.05	April 1, 2024
CA#3 CA#4	Security Communication RootCA Subordinate CA Certificate Policy	6.04	January 24, 2024
CA#5 CA#6	Security Communication RootCA Subordinate CA Certificate Policy	6.03	July 11, 2023
	Security Communication RootCA Subordinate CA Certificate Policy	6.02	May 17, 2023
CA#1 CA#2 CA#3	Security Communication RootCA Time-Stamp Service Certificate Policy	5.09	January 24, 2024
CA#4 CA#5 CA#6	Security Communication RootCA Time-Stamp Service Certificate Policy	5.08	May 17, 2023
CA#7	SECOM Passport for Web SR Certification Authority Certificate Policy	3.04	April 1, 2024
	SECOM Passport for Web SR Certification Authority Certificate Policy	3.03	August 28, 2023
	SECOM Passport for Web SR Certification Authority Certificate Policy	3.02	May 17, 2023
CA#8	Organization Validation Certificate Policy	1.22	April 1, 2024
CA#9	Organization Validation Certificate Policy	1.21	August 28, 2023
CA#10	Organization Validation Certificate Policy	1.20	May 17, 2023
CA#11	SECOM Passport for Web EV Certification Authority Certificate Policy	3.04	April 1, 2024
	SECOM Passport for Web EV Certification Authority Certificate Policy	3.03	September 14, 2023
	SECOM Passport for Web EV Certification Authority Certificate Policy	3.02	August 28, 2023
	SECOM Passport for Web EV Certification Authority Certificate Policy	3.01	May 17, 2023
CA#12 CA#13	SECOM Passport for Member 2.0 PUB Certificate Policy	6.07	May 17, 2024
CA#14 CA#15	SECOM Passport for Member 2.0 PUB Certificate Policy	6.06	April 1, 2024
CA#16 CA#17	SECOM Passport for Member 2.0 PUB Certificate Policy	6.05	August 28, 2023
CA#18 CA#19	SECOM Passport for Member 2.0 PUB Certificate Policy	6.04	May 17, 2023
CA#20 CA#21	Sumitomo Mitsui Banking Corporation's Digital Contract Service Certificate Policy / Certification Practices Statement	1.5	May 1, 2023



(Translation)

CA#22	SECOM TimeStamping CA Time-Stamp Service Certificate Policy	5.07	July 12, 2024
CA#23			
CA#24	SECOM TimeStamping CA Time-Stamp Service Certificate Policy	5.06	April 1, 2024
	SECOM TimeStamping CA Time-Stamp Service Certificate Policy	5.05	May 17, 2023
CA#25	Domain Validation Certificate Policy	1.22	April 1, 2024
CA#26	Domain Validation Certificate Policy	1.21	August 28, 2023
	Domain Validation Certificate Policy	1.20	May 17, 2023

Certification Practice Statement

CA	Policy Name	Version	Date
CA#1	Security Communication RootCA Certification Practice Statement	6.04	April 1, 2024
CA#2			
CA#3	Security Communication RootCA Certification Practice Statement	6.03	January 24, 2024
CA#4			
CA#5	Security Communication RootCA Certification Practice Statement	6.02	May 17, 2023
CA#6			
CA#7	SECOM Digital Certification Infrastructure Certification Practice Statement	2.19	April 1, 2024
CA#8			
CA#9			
CA#10			
CA#11			
CA#12			
CA#13			
CA#14			
CA#15			
CA#16	SECOM Digital Certification Infrastructure Certification Practice Statement	2.18	May 17, 2023
CA#17			
CA#18			
CA#19			
CA#22			
CA#23			
CA#24			
CA#25			
CA#26			
CA#20	Sumitomo Mitsui Banking Corporation's Digital Contract Service Certificate Policy / Certification Practices Statement	1.5	May 1, 2023
CA#21			



(Translation)

APPENDIX C

#	Disclosure	Publicly Disclosed Link
1	SECOM: Certificates Issued with lower case value in subject:countryName	https://bugzilla.mozilla.org/show_bug.cgi?id=1896596
2	SECOM: Difference in upper and lower case between CN field and SAN	https://bugzilla.mozilla.org/show_bug.cgi?id=1897346

(Translation)

STS MANAGEMENT'S ASSERTION

August 26, 2024

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.

(Translation)

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 June 7, 2023 to June 6, 2024, 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
- 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 has enumerated the information to [Appendix C](#), that have been posted publicly on Bugzilla's site which is the online forums of individual internet browsers that comprise the CA/Browser Forum.

Appendix A, #1-1 CAs was revoked on September 30, 2023.

Appendix A, #13-2 CAs was revoked on November 20, 2023.

Appendix A, #23-2 CAs did not issue certificates during the period November 11, 2023 to November 16, 2023 and were maintained online to provide revocation status information only.

Those CAs were also revoked on November 16, 2023.

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: Security Communication RootCA1
CA#2: Security Communication RootCA2
CA#3: Security Communication RootCA3
CA#4: Security Communication ECCRootCA1
CA#5: SECOM RSA Root CA 2023
CA#6: SECOM Document Signing RSA Root CA 2023
OV SSL Issuing CAs
CA#7: SECOM Passport for Web SR 3.0 CA
CA#8: NII Open Domain CA - G7 RSA
CA#9: NII Open Domain CA - G7 ECC
CA#10: CrossTrust OV CA5
EV SSL Issuing CAs
CA#11: SECOM Passport for Web EV 2.0 CA
Non-EV Code Signing Issuing CAs
CA#12: SECOM Passport for CodeSigning CA G2
Secure Email (S/MIME) CAs
CA#13: SECOM Passport for Member PUB CA4
CA#14: SECOM Passport for Member PUB CA5
CA#15: SECOM Passport for Member PUB CA8
CA#16: SECOM Passport for PublicID SMIME RSA CA 2023
Document Signing CAs
CA#17: SECOM Passport for Member PUB CA7
CA#18: SECOM Passport for PublicID Document Signing RSA CA 2023
CA#19: SECOM Passport for PublicID AATL RSA CA 2023

(Translation)

CA#20: SMBC Certificate Authority CA2
CA#21: SMBC Certificate Authority CA2 G2
Timestamp CAs
CA#22: SECOM TimeStamping CA3
CA#23: SECOM TimeStamping CA4
CA#24: SECOM TimeStamping CA2
Other CAs
CA#25: CrossTrust DV CA5
CA#26: FujiSSL Public Validation Authority - G3

CA Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
1	1	OU = Security Communication RootCA1 O = SECOM Trust.net C = JP	OU = Security Communication RootCA1 O = SECOM Trust.net C = JP	00	rsaEncryption	2048bit	sha1WithRSAEncryption	Sep 30 04:20:49 2003 GMT	Sep 30 04:20:49 2023 GMT	A073499968DC855B65E39B282F579FBD33BC0748	E75E72ED9F560EEC6EB4800073A43FC3AD19195A392282017895974A99026B6C	
2	1	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	00	rsaEncryption	2048bit	sha256WithRSAEncryption	May 29 05:00:39 2009 GMT	May 29 05:00:39 2029 GMT	0A85A9776505987C4081F80F972C38F10AEC3CCF	513B2CECB810D4CDE5DD85391ADFC6C2DD60D87BB736D2B521484AA47A0EBEF6	2.23.140.1.2.1 2.23.140.1.2.2 2.23.140.1.1 2.23.140.1.4.1 2.23.140.1.5.1.3
3	1	OU = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	00E17C3740FD1BFE67	rsaEncryption	4096bit	sha384WithRSAEncryption	Jun 16 06:17:16 2016 GMT	Jan 18 06:17:16 2038 GMT	64147CFC587216A60A2934156F2ACBBCFCAFA8AB	24A55C2AB051442D0617766541239A4AD032D7C55175AA34FFDE2FBC4F5C5294	2.23.140.1.4.1 2.23.140.1.4.2
4	1	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	00D65D9BB378812EEB	ECDSAEncryption	384bit	sha384WithECDSAEncryption	Jun 16 05:15:28 2016 GMT	Jan 18 05:15:28 2038 GMT	861CE7FE2DA54A8B08FE2811FABEA366F860592F	E74FBDA55BD564C473A36B441AA799C8A68E077440E8288B9FA1E50E4BBACA11	2.23.140.1.2.1 2.23.140.1.2.2
4	2	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B1A49DB1D47C2674294CEE84F8FC	ECDSAEncryption	384bit	sha384WithECDSAEncryption	Apr 4 06:22:18 2024 GMT	May 29 05:00:39 2029 GMT	861CE7FE2DA54A8B08FE2811FABEA366F860592F	C3EBCEA7E6B13AC3EB3A79F05819E67D6893C65642F50D9B5E1647CB26506B8E	2.23.140.1.2.1 2.23.140.1.2.2

(Translation)

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
5	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	51336A2AEFDB1F80EDB2C6D306D22593C4C8B666	2C154235528D701790B675AFF6E1970827B10ED665E913835BF46E3460FD5C84	-
6	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	-
7	1	CN = SECOM Passport for Web SR 3.0 CA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B12F4D05F9ED13	rsaEncryption	2048bit	sha256WithRSAEncryption	Mar 16 05:49:12 2018 GMT	Mar 16 05:49:12 2028 GMT	CBEF3DEF8374A1A842F03B4036FA6D8294A92736	E05ED4A9E4C773308A93E849861225AE349A92BBD4BACDD4900AD4E73B131100	2.23.140.1.2.2
8	1	CN = NII Open Domain CA - G7 RSA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18587A69943B5EC368F4CAF68F7	rsaEncryption	2048bit	sha256WithRSAEncryption	Dec 15 08:46:22 2020 GMT	May 29 05:00:39 2029 GMT	B02EE551EDFC4ACFA387F11390762D9D8E94A1E3	603DB707A584003BED6F1D43DCD4EAE13CD18D798E827DE2F3A31F3193FC0DAC	2.23.140.1.2.2
9	1	CN=NII Open Domain CA - G7 ECC O=SECOM Trust Systems CO.,LTD. C=JP	CN=Security Communication ECC RootCA1 O=SECOM Trust Systems CO.,LTD. C=JP	0100004C9F5DEB113CD4FB41C8C9EC7D	ECDSAEncryption	384bit	sha384WithECDSAEncryption	Dec 15 09:17:38 2020 GMT	Dec 15 09:17:38 2030 GMT	6B30200CAEB7C3139BD9A759178A5E30C14C5549	81CD03067252FFE849B240DCC24566678677E3F5FEDC4C540D7A26CAD2C081C8	2.23.140.1.2.2

(Translation)

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
10	1	CN = CrossTrust OV CA5 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B152643B 58B011	rsaEncr yption	2048bit	sha256With RSAEncryp tion	Aug 22 07:23:58 2018 GMT	Aug 22 07:23:58 2028 GMT	24B7B441D4324F C419FF5E62643B 5E69276117DC	79C4091B05B15C1683128B7A355E0AAD62E1BBBC3E5F3735370C6CC4D1AFB44	2.23.140.1.2.2
11	1	CN = SECOM Passport for Web EV 2.0 CA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B0C9	rsaEncr yption	2048bit	sha256With RSAEncryp tion	Dec 16 07:04:09 2014 GMT	Dec 16 07:04:09 2024 GMT	164BFB0C97388 A185A54A146CF 892447CCC476B3	E1F2E95000F815E11C81490430B5D02C8D81D0D256C85DF68B516D6C27761926	2.23.140.1.1
11	2	CN = SECOM Passport for Web EV 2.0 CA O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B19D60F2 A361D7FA7E9 57C63BD5C	rsaEncr yption	2048bit	sha256With RSAEncryp tion	Aug 30 04:35:47 2023 GMT	May 29 05:00:39 2029 GMT	164BFB0C97388 A185A54A146CF 892447CCC476B3	39B6E3B388F749521DF2B354182EB4CD87D4BF36439BFAF0202E5596CFC2CAA4	2.23.140.1.1
12	1	CN = SECOM Passport for CodeSigning CA G2 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100004ECD64 452CBAA77EE 74E33D048	rsaEncr yption	4096bit	sha384With RSAEncryp tion	May 25 01:37:39 2021 GMT	May 25 01:37:39 2031 GMT	4C6C10EB253A4 893C35BBE3DB6 8CFB9EFDB64A6 5	BB974448A25466F597A55772577FD6C69FDC4D9F8D2B2D8A0232D04E77D52C8C	2.23.140.1.4.1
12	2	CN = SECOM Passport for CodeSigning CA G2 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B180E465 8AB862062FC7 602DB247	rsaEncr yption	4096bit	sha256With RSAEncryp tion	Aug 6 08:53:55 2020 GMT	May 29 05:00:39 2029 GMT	4C6C10EB253A4 893C35BBE3DB6 8CFB9EFDB64A6 5	2A2AC8DE79A38177699A34FA06D3E5FB86C27CDD0CAF3B332C8D861D0A753639	2.23.140.1.4.1

(Translation)

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
13	1	CN = SECOM Passport for Member PUB CA4 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B1575075 487009	rsaEncryption	2048bit	sha256With RSAEncryption	Oct 4 05:28:09 2018 GMT	Oct 4 05:28:09 2028 GMT	488C6576D21EA BF5FF3824B6C43 6D90A9FA0BCA E	B10861737B3EC9B11FA6154D23970FFB2DABFC28AE6A6BF56C3F3204266239AD	-
13	2	CN = SECOM Passport for Member PUB CA4 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B0BC	rsaEncryption	2048bit	sha256With RSAEncryption	Nov 20 02:18:46 2013 GMT	Nov 20 02:18:46 2023 GMT	488C6576D21EA BF5FF3824B6C43 6D90A9FA0BCA E	0940451DFECB675B5204C8AE07189D4E4E90957CFD2BAFDCFF36DB20C279E91A	-
14	1	CN = SECOM Passport for Member PUB CA5 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B16DA7E 6F3BBBA	rsaEncryption	2048bit	sha256With RSAEncryption	May 20 07:10:35 2020 GMT	May 29 05:00:39 2029 GMT	8939416491E946 A4165907F22BA F527F7D4BDA92	8C6DB8171AE6785F05426AE58C3D36F7559352202E9209B9D29B1BD447961DC8	-
14	2	CN = SECOM Passport for Member PUB CA5 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B0E1D249 6D57C4	rsaEncryption	2048bit	sha256With RSAEncryption	Aug 12 04:48:29 2015 GMT	Aug 12 04:48:29 2025 GMT	8939416491E946 A4165907F22BA F527F7D4BDA92	C931A0F85A052901234A54FD460D417F1A8B63C38C4811F79B98F3AE1C2FE9FB	-
15	1	CN = SECOM Passport for Member PUB CA8 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B12B288 A041897	rsaEncryption	2048bit	sha256With RSAEncryption	Jan 9 06:01:29 2018 GMT	Jan 9 06:01:29 2028 GMT	762BD98DCC353 6324505DF9E8C6 A17D133DC0307	7A4FCBA079F5BDDCF0A76C3B03A377E155A53009474A1B3EB8F34961A53BDA9C	-

(Translation)

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
16	1	CN = SECOM Passport for PublicID SMIME RSA CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B19AF3380D8F037998731AA1D930	rsaEncryption	4096bit	sha384WithRSAEncryption	Jun 7 04:33:22 2023 GMT	May 29 05:00:39 2029 GMT	0136A8AB68C0C698FA996CC6A4FA92A83714E2D2	DB088F140ACBE85FA1EC83D3851063803FFD8471564CF852B92A60FEB965A02F	2.23.140.1.5.1.3
17	1	CN = SECOM Passport for Member PUB CA7 OU = SECOM Passport for Member 2.0 PUB O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18CA7598FE1D7178D0169AC380F	rsaEncryption	2048bit	sha256WithRSAEncryption	Jul 12 06:32:24 2021 GMT	May 29 05:00:39 2029 GMT	BD085E25849CFD3524D81DC7306C789DC1A4BB20	BA08827159A8510FDF274383DCC44E70423416DF862B972F8945AAF49E30D5A4	-
18	1	CN = SECOM Passport for PublicID Document Signing RSA CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM RSA Root CA 2023 O = SECOM Trust Systems Co., Ltd. C = JP	010000041C223AF622A83408EB6D397D	rsaEncryption	4096bit	sha384WithRSAEncryption	Feb 24 06:53:38 2023 GMT	Feb 1 00:00:00 2043 GMT	B72166C25545E7934EA2C8AD5DB4063242CEE1D9	368A62B89C9713662E409AB7DF722525D6B226551B518F960559EE1DF0FFA16E	-

(Translation)

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
19	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 RSAEncryp tion	Feb 24 07:41:36 2023 GMT	Feb 1 00:00:00 2043 GMT	8939416491E946 A4165907F22BA F527F7D4BDA92	D2A60B7C6DFE267AD055DA26BF68D9F1478D862310F3DD0A73325941C2F00DDE	-
20	1	CN = SMBC Certificate Authority CA2 OU = SMBC Authority O = Sumitomo Mitsui Banking Corporation C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18FB4B 469F41224BD4 D771CD48F	rsaEncr yption	2048bit	sha256With RSAEncryp tion	Aug 13 05:45:33 2021 GMT	May 29 05:00:39 2029 GMT	5F2B8D9DBA6B 0CADE15F17616 448A0952A96F08 7	7B2EE6E46480EE7C43F759D45BEDBD3D7A5BEDEE8B888CEAAB3D811644AC4682	-
21	1	CN = SMBC Certificate Authority CA2 G2 OU = SMBC Authority O = Sumitomo Mitsui Banking Corporation C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100004AF024 24DAF397BD4 AEA6B8D10	rsaEncr yption	2048bit	sha384With RSAEncryp tion	Nov 6 05:09:15 2020 GMT	Dec 31 14:59:59 2030 GMT	0DA7566D6FE3C EA31BAADB025 2F7109D314442F F	FB6F8CF1EB756CB6C1E61571CADADC46FFA8871F686CAAE0F775B25A8B8AD701	-
22	1	CN = SECOM TimeStamping CA3 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100003E344C 91C7CC	rsaEncr yption	4096bit	sha384With RSAEncryp tion	Jun 7 05:12:31 2018 GMT	Dec 31 05:12:31 2037 GMT	199DFABC5C345 5AF3CC59B4DB BA3A5963928884 4	0E984339724A267C2A3DC4FCC8D020B3B4BA329A0AD7E390CFBF76E88823E11B	-
23	1	CN = SECOM TimeStamping CA4 O = SECOM Trust Systems CO.,LTD. C = JP	CN = Security Communication RootCA3 O = SECOM Trust Systems CO.,LTD. C = JP	0100004BD4F4 9CF31A08CB1 F6953D0DD	rsaEncr yption	4096bit	sha384With RSAEncryp tion	Dec 15 09:48:40 2020 GMT	Dec 31 14:59:59 2037 GMT	60811F0DE823D C6EB01949BEE7 F90D2448C19DB 6	3CFC266D4E23BCF70E99CC7918ED578A300498F00C8BBD123250BDEE5A2BEC5B	2.23.140.1.4.2

(Translation)

Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
23	2 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	60811F0DE823DC6EB01949BEE7F90D2448C19DB6	9B7A75CCF8D0EDAC6088D40F14B6D20C85C69B2B7F5A2C957FB1C2BC5870BAF5	-
24	1 CN = SECOM TimeStamping CA2 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B18D4E99D73CB4EC2BEA646E1AE6	rsaEncryption	2048bit	sha256WithRSAEncryption	Jul 12 06:47:19 2021 GMT	May 29 05:00:39 2029 GMT	074D137DEAB7FAED93D493773F581300CBE12389	2AF80BCD3A5A53406FF22271DB84B938417E8C338E5AA28CC47575FD41F22615	-
25	1 CN = CrossTrust DV CA5 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B15323E5AEFDCD	rsaEncryption	2048bit	sha256WithRSAEncryption	Aug 22 07:32:24 2018 GMT	Aug 22 07:32:24 2028 GMT	4F8B70CFA9401C96E5945D77ACD66F4D2D9BF277	18F4368FE93B3CAE025230BCE7EAD340FD90FB27F9A10E36FEE89FC454F22788	2.23.140.1.2.1
26	1 CN = FujiSSL Public Validation Authority - G3 O = SECOM Trust Systems CO.,LTD. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B154F33C5E5E00	rsaEncryption	2048bit	sha256WithRSAEncryption	Aug 22 07:41:02 2018 GMT	Aug 22 07:41:02 2028 GMT	BCBED911E051646FFFF0744F0D5AAB4A4F2D7827	56DA6EFEF1D504134C72EEDC3AE44AA7FA11B848820DBFAA86CA8E35D60EDB04	2.23.140.1.2.1

APPENDIX B

Certificate Policy

CA	Policy Name	Version	Date
CA#1 CA#2	Security Communication RootCA Subordinate CA Certificate Policy	6.05	April 1, 2024
CA#3 CA#4	Security Communication RootCA Subordinate CA Certificate Policy	6.04	January 24, 2024
CA#5 CA#6	Security Communication RootCA Subordinate CA Certificate Policy	6.03	July 11, 2023
	Security Communication RootCA Subordinate CA Certificate Policy	6.02	May 17, 2023
CA#1 CA#2 CA#3	Security Communication RootCA Time-Stamp Service Certificate Policy	5.09	January 24, 2024
CA#4 CA#5 CA#6	Security Communication RootCA Time-Stamp Service Certificate Policy	5.08	May 17, 2023
CA#7	SECOM Passport for Web SR Certification Authority Certificate Policy	3.04	April 1, 2024
	SECOM Passport for Web SR Certification Authority Certificate Policy	3.03	August 28, 2023
	SECOM Passport for Web SR Certification Authority Certificate Policy	3.02	May 17, 2023
CA#8 CA#9 CA#10	Organization Validation Certificate Policy	1.22	April 1, 2024
	Organization Validation Certificate Policy	1.21	August 28, 2023
	Organization Validation Certificate Policy	1.20	May 17, 2023
CA#11	SECOM Passport for Web EV Certification Authority Certificate Policy	3.04	April 1, 2024
	SECOM Passport for Web EV Certification Authority Certificate Policy	3.03	September 14, 2023
	SECOM Passport for Web EV Certification Authority Certificate Policy	3.02	August 28, 2023
	SECOM Passport for Web EV Certification Authority Certificate Policy	3.01	May 17, 2023
CA#12 CA#13 CA#14 CA#15 CA#16 CA#17 CA#18 CA#19	SECOM Passport for Member 2.0 PUB Certificate Policy	6.07	May 17, 2024
	SECOM Passport for Member 2.0 PUB Certificate Policy	6.06	April 1, 2024
	SECOM Passport for Member 2.0 PUB Certificate Policy	6.05	August 28, 2023
	SECOM Passport for Member 2.0 PUB Certificate Policy	6.04	May 17, 2023
CA#20 CA#21	Sumitomo Mitsui Banking Corporation's Digital Contract Service Certificate Policy / Certification Practices Statement	1.5	May 1, 2023

(Translation)

CA#22	SECOM TimeStamping CA Time-Stamp Service Certificate Policy	5.07	July 12, 2024
CA#23			
CA#24	SECOM TimeStamping CA Time-Stamp Service Certificate Policy	5.06	April 1, 2024
	SECOM TimeStamping CA Time-Stamp Service Certificate Policy	5.05	May 17, 2023
CA#25	Domain Validation Certificate Policy	1.22	April 1, 2024
CA#26	Domain Validation Certificate Policy	1.21	August 28, 2023
	Domain Validation Certificate Policy	1.20	May 17, 2023

Certification Practice Statement

CA	Policy Name	Version	Date
CA#1	Security Communication RootCA Certification Practice Statement	6.04	April 1, 2024
CA#2			
CA#3	Security Communication RootCA Certification Practice Statement	6.03	January 24, 2024
CA#4			
CA#5			
CA#6	Security Communication RootCA Certification Practice Statement	6.02	May 17, 2023
CA#7	SECOM Digital Certification Infrastructure Certification Practice Statement	2.19	April 1, 2024
CA#8			
CA#9			
CA#10			
CA#11			
CA#12			
CA#13			
CA#14			
CA#15			
CA#16	SECOM Digital Certification Infrastructure Certification Practice Statement	2.18	May 17, 2023
CA#17			
CA#18			
CA#19			
CA#22			
CA#23			
CA#24			
CA#25			
CA#26			
CA#20	Sumitomo Mitsui Banking Corporation's Digital Contract Service Certificate Policy / Certification Practices Statement	1.5	May 1, 2023
CA#21			

(Translation)

APPENDIX C

#	Disclosure	Publicly Disclosed Link
1	SECOM: Certificates Issued with lower case value in subject:countryName	https://bugzilla.mozilla.org/show_bug.cgi?id=1896596
2	SECOM: Difference in upper and lower case between CN field and SAN	https://bugzilla.mozilla.org/show_bug.cgi?id=1897346