



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-EV 保証規準 v1.8 \(the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.8\)](#) 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 ブラウザフォーラムガイドラインに準拠して Extended Validation SSL（以下「EV SSL」という。）証明書を提供するためのコミットメントを含む EV SSL 証明書ライフサイクル管理のビジネス実務を、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、当該開示された実務に従ってサービスを提供していた。
- 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ための有効な内部統制を維持していた。
  - 管理する鍵と EV SSL 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。
  - EV SSL 加入者情報は、（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。

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。



## 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-EV 保証規準 v1.8](#) 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 EV SSL 証明書の発行、更新、失効にわたる関連する内部統制を含む EV SSL 証明書ライフサイクル管理のビジネス実務を理解すること、(2) セコムトラストシステムズ株式会社が開示した EV SSL 証明書ライフサイクル管理の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-EV 保証規準 v1.8](#) 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-EV 保証規準 v1.8](#) 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-EV 保証規準シールの使用は、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

<b>Root CAs</b>
CA#1: Security Communication RootCA1
CA#2: Security Communication RootCA2
<b>EV SSL Issuing CAs</b>
CA#3: SECOM Passport for Web EV 2.0 CA



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	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
3	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	39B6E3B388F749521DF2B354182EB4CD87D4BF36439BFAF0202E5596CFC2CAA4	2.23.140.1.1



付録 B

証明書ポリシー

CA	CP 名	Version	日付
CA#1 CA#2	<a href="#">Security Communication RootCA 下位 CA 用証明書ポリシー</a>	6.05	2024/4/1
	<a href="#">Security Communication RootCA 下位 CA 用証明書ポリシー</a>	6.04	2024/1/24
	<a href="#">Security Communication RootCA 下位 CA 用証明書ポリシー</a>	6.03	2023/7/11
	<a href="#">Security Communication RootCA 下位 CA 用証明書ポリシー</a>	6.02	2023/5/17
CA#1 CA#2	<a href="#">Security Communication RootCA タイムスタンプサービス用証明書ポリシー</a>	5.09	2024/1/24
	<a href="#">Security Communication RootCA タイムスタンプサービス用証明書ポリシー</a>	5.08	2023/5/17
CA#3	<a href="#">セコムパスポート for Web EV 認証局証明書ポリシー</a>	3.04	2024/4/1
	<a href="#">セコムパスポート for Web EV 認証局証明書ポリシー</a>	3.03	2023/9/14
	<a href="#">セコムパスポート for Web EV 認証局証明書ポリシー</a>	3.02	2023/8/28
	<a href="#">セコムパスポート for Web EV 認証局証明書ポリシー</a>	3.01	2023/5/17

運用規程

CA	CPS 名	Version	日付
CA#1 CA#2	<a href="#">Security Communication RootCA 認証運用規定</a>	6.04	2024/4/1
	<a href="#">Security Communication RootCA 認証運用規定</a>	6.03	2024/1/24
	<a href="#">Security Communication RootCA 認証運用規定</a>	6.02	2023/5/17
CA#3	<a href="#">セコム電子認証基盤認証運用規程</a>	2.19	2024/4/1
	<a href="#">セコム電子認証基盤認証運用規程</a>	2.18	2023/5/17



付録 C

#	開示内容	公開リンク
1	SECOM: Certificates Issued with lower case value in subject:countryName	<a href="https://bugzilla.mozilla.org/show_bug.cgi?id=1896596">https://bugzilla.mozilla.org/show_bug.cgi?id=1896596</a>

## 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

横澤 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、Extended Validation SSL（以下「EV SSL」という。）CA サービスを提供している。

当社の経営者は、当社の Web サイトで公開している EV SSL CA ビジネス実務の開示、EV SSL 鍵ライフサイクル管理の内部統制、及び EV SSL 証明書ライフサイクル管理の内部統制を含む当社の EV SSL 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 EV SSL CA サービス（東京）に関する証明書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、[認証局のための WebTrust-EV 保証規準 v1.8 \(the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.8\)](#) 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、EV SSL CA サービスの提供に関して、下記の事項を実施した。

- CA ブラウザフォーラムガイドラインに準拠して EV SSL 証明書を提供するためのコミットメントを含む EV SSL 証明書ライフサイクル管理のビジネス実務を、当社のウェブサイト上で[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、当該開示された実務に従ってサービスを提供していた。
- 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。
  - 管理する鍵と EV SSL 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。
  - EV SSL 加入者情報は、（当社が行う登録業務のため）適切に認証されていたこと。

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。

付録 A

対象CA

<b>Root CAs</b>
CA#1: Security Communication RootCA1
CA#2: Security Communication RootCA2
<b>EV SSL Issuing CAs</b>
CA#3: SECOM Passport for Web EV 2.0 CA

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	デ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
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	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
3	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	39B6E3B388F749521DF2B354182EB4CD87D4BF36439BF0202E5596CFC2CAA4	2.23.140.1.1

付録 B

証明書ポリシー

CA	CP 名	Version	日付
CA#1 CA#2	<a href="#">Security Communication RootCA 下位 CA 用証明書ポリシー</a>	6.05	2024/4/1
	<a href="#">Security Communication RootCA 下位 CA 用証明書ポリシー</a>	6.04	2024/1/24
	<a href="#">Security Communication RootCA 下位 CA 用証明書ポリシー</a>	6.03	2023/7/11
	<a href="#">Security Communication RootCA 下位 CA 用証明書ポリシー</a>	6.02	2023/5/17
CA#1 CA#2	<a href="#">Security Communication RootCA タイムスタンプサービス用証明書ポリシー</a>	5.09	2024/1/24
	<a href="#">Security Communication RootCA タイムスタンプサービス用証明書ポリシー</a>	5.08	2023/5/17
CA#3	<a href="#">セコムパスポート for Web EV 認証局証明書ポリシー</a>	3.04	2024/4/1
	<a href="#">セコムパスポート for Web EV 認証局証明書ポリシー</a>	3.03	2023/9/14
	<a href="#">セコムパスポート for Web EV 認証局証明書ポリシー</a>	3.02	2023/8/28
	<a href="#">セコムパスポート for Web EV 認証局証明書ポリシー</a>	3.01	2023/5/17

運用規程

CA	CPS 名	Version	日付
CA#1 CA#2	<a href="#">Security Communication RootCA 認証運用規定</a>	6.04	2024/4/1
	<a href="#">Security Communication RootCA 認証運用規定</a>	6.03	2024/1/24
	<a href="#">Security Communication RootCA 認証運用規定</a>	6.02	2023/5/17
CA#3	<a href="#">セコム電子認証基盤認証運用規程</a>	2.19	2024/4/1
	<a href="#">セコム電子認証基盤認証運用規程</a>	2.18	2023/5/17

付録 C

#	開示内容	公開リンク
1	SECOM: Certificates Issued with lower case value in subject:countryName	<a href="https://bugzilla.mozilla.org/show_bug.cgi?id=1896596">https://bugzilla.mozilla.org/show_bug.cgi?id=1896596</a>

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 extended validation SSL ("EV SSL") certificate lifecycle management business practices in its Certification Practice Statements and Certificate Policies enumerated in [Appendix B](#), including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the STS website, and provided such services in accordance with its disclosed practices
2. maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by STS)

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#).

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



(Translation)

### **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 – Extended Validation SSL v1.8](#).

### **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 EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;
- (2) selectively testing transactions executed in accordance with disclosed EV SSL certificate lifecycle management 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.

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.



(Translation)

**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 – Extended Validation SSL v1.8](#).

This report does not include any representation as to the quality of STS’s CA services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#), 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 – Extended Validation SSL 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

<b>Root CAs</b>
CA#1: Security Communication RootCA1
CA#2: Security Communication RootCA2
<b>EV SSL Issuing CAs</b>
CA#3: SECOM Passport for Web EV 2.0 CA



(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	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
3	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	39B6E3B388F749521DF2B354182EB4CD87D4BF36439BFAF0202E5596CFC2CAA4	2.23.140.1.1



(Translation)

**APPENDIX B**

**Certificate Policy**

CA	Policy Name	Version	Date
CA#1 CA#2	<a href="#">Security Communication RootCA Subordinate CA Certificate Policy</a>	6.05	April 1, 2024
	<a href="#">Security Communication RootCA Subordinate CA Certificate Policy</a>	6.04	January 24, 2024
	<a href="#">Security Communication RootCA Subordinate CA Certificate Policy</a>	6.03	July 11, 2023
	<a href="#">Security Communication RootCA Subordinate CA Certificate Policy</a>	6.02	May 17, 2023
CA#1 CA#2	<a href="#">Security Communication RootCA Time-Stamp Service Certificate Policy</a>	5.09	January 24, 2024
	<a href="#">Security Communication RootCA Time-Stamp Service Certificate Policy</a>	5.08	May 17, 2023
CA#3	<a href="#">SECOM Passport for Web EV Certification Authority Certificate Policy</a>	3.04	April 1, 2024
	<a href="#">SECOM Passport for Web EV Certification Authority Certificate Policy</a>	3.03	September 14, 2023
	<a href="#">SECOM Passport for Web EV Certification Authority Certificate Policy</a>	3.02	August 28, 2023
	<a href="#">SECOM Passport for Web EV Certification Authority Certificate Policy</a>	3.01	May 17, 2023

**Certification Practice Statement**

CA	Policy Name	Version	Date
CA#1 CA#2	<a href="#">Security Communication RootCA Certification Practice Statement</a>	6.04	April 1, 2024
	<a href="#">Security Communication RootCA Certification Practice Statement</a>	6.03	January 24, 2024
	<a href="#">Security Communication RootCA Certification Practice Statement</a>	6.02	May 17, 2023
CA#3	<a href="#">SECOM Digital Certification Infrastructure Certification Practice Statement</a>	2.19	April 1, 2024
	<a href="#">SECOM Digital Certification Infrastructure Certification Practice Statement</a>	2.18	May 17, 2023



(Translation)

**APPENDIX C**

#	Disclosure	Publicly Disclosed Link
1	SECOM: Certificates Issued with lower case value in subject:countryName	<a href="https://bugzilla.mozilla.org/show_bug.cgi?id=1896596">https://bugzilla.mozilla.org/show_bug.cgi?id=1896596</a>

## 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 Extended Validation SSL ("EV SSL") CA services.

The management of STS is responsible for establishing and maintaining effective controls over its EV SSL CA operations, including its EV SSL CA business practices disclosure on its website, EV SSL key lifecycle management controls, and EV SSL 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 EV SSL CA services. Based on that assessment, in STS management's opinion, in providing its EV SSL CA services at Tokyo, Japan, throughout the period June 7, 2023 to June 6, 2024, STS has:

1. disclosed its EV SSL certificate lifecycle management business practices in its Certification Practice Statements and Certificate Policies enumerated in [Appendix B](#), including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the STS website, and provided such services in accordance with its disclosed practices
2. maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and

*(Translation)*

- EV SSL subscriber information is properly authenticated (for the registration activities performed by STS)

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#).

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.

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

## APPENDIX A

### List of CAs in Scope

<b>Root CAs</b>
CA#1: Security Communication RootCA1
CA#2: Security Communication RootCA2
<b>EV SSL Issuing CAs</b>
CA#3: SECOM Passport for Web EV 2.0 CA

(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	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
3	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	39B6E3B388F749521DF2B354182EB4CD87D4BF36439BFAF0202E5596CFC2CAA4	2.23.140.1.1

**APPENDIX B**

## Certificate Policy

CA	Policy Name	Version	Date
CA#1 CA#2	<a href="#">Security Communication RootCA Subordinate CA Certificate Policy</a>	6.05	April 1, 2024
	<a href="#">Security Communication RootCA Subordinate CA Certificate Policy</a>	6.04	January 24, 2024
	<a href="#">Security Communication RootCA Subordinate CA Certificate Policy</a>	6.03	July 11, 2023
	<a href="#">Security Communication RootCA Subordinate CA Certificate Policy</a>	6.02	May 17, 2023
CA#1 CA#2	<a href="#">Security Communication RootCA Time-Stamp Service Certificate Policy</a>	5.09	January 24, 2024
	<a href="#">Security Communication RootCA Time-Stamp Service Certificate Policy</a>	5.08	May 17, 2023
CA#3	<a href="#">SECOM Passport for Web EV Certification Authority Certificate Policy</a>	3.04	April 1, 2024
	<a href="#">SECOM Passport for Web EV Certification Authority Certificate Policy</a>	3.03	September 14, 2023
	<a href="#">SECOM Passport for Web EV Certification Authority Certificate Policy</a>	3.02	August 28, 2023
	<a href="#">SECOM Passport for Web EV Certification Authority Certificate Policy</a>	3.01	May 17, 2023

## Certification Practice Statement

CA	Policy Name	Version	Date
CA#1 CA#2	<a href="#">Security Communication RootCA Certification Practice Statement</a>	6.04	April 1, 2024
	<a href="#">Security Communication RootCA Certification Practice Statement</a>	6.03	January 24, 2024
	<a href="#">Security Communication RootCA Certification Practice Statement</a>	6.02	May 17, 2023
CA#3	<a href="#">SECOM Digital Certification Infrastructure Certification Practice Statement</a>	2.19	April 1, 2024
	<a href="#">SECOM Digital Certification Infrastructure Certification Practice Statement</a>	2.18	May 17, 2023

(Translation)

### APPENDIX C

#	Disclosure	Publicly Disclosed Link
1	SECOM: Certificates Issued with lower case value in subject:countryName	<a href="https://bugzilla.mozilla.org/show_bug.cgi?id=1896596">https://bugzilla.mozilla.org/show_bug.cgi?id=1896596</a>