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

INDEPENDENT ASSURANCE REPORT

July 28, 2026

To the management of SECOM Trust Systems Co., Ltd. ("STS"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on STS management's assertion that for its Certification Authority (CA) operations at its locations as detailed in Appendix A, throughout the period June 7, 2025 to June 6, 2026 for its CAs as enumerated in Appendix B, STS has:

1. disclosed its TLS certificate lifecycle management business practices in its Certification Practice Statements and Certificate Policies enumerated in Appendix C, including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirements 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 TLS certificates it manages is established and protected throughout their lifecycles; and
   - TLS subscriber information is properly authenticated (for the registration activities performed by STS)

3. 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 - TLS Baseline v2.9.

The CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates require the CA to operate controls to adhere to the Network and Certificate System Security Requirements. The WebTrust Principles and Criteria for Certification Authorities - Network Security address this requirement and are reported on in a separate report.

Appendix B, #14-1 CA did not issue certificates during the period June 7, 2025 to March 5, 2026 and was maintained online to provide revocation status information only. That CA was revoked on March 5, 2026.

KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

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 - TLS Baseline v2.9.

Our independence and quality management
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, Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements, which requires the firm to design, implement and operate a system of quality management including documented policies or 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 TLS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of TLS certificates;
(2) selectively testing transactions executed in accordance with disclosed TLS 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 unauthorized 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, 2025 to June 6, 2026, 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 - TLS Baseline v2.9.

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 - TLS Baseline v2.9, 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 - TLS Baseline 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 D and Appendix E, 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 other matter described in Appendix E relates to a Bugzilla incident arising from the operation of an externally operated subordinate CA, which is outside the scope of this report, and was therefore not subject to our analysis of Bugzilla issues described below.

Without modifying our opinion, we noted the following other matters described in Appendix D during our procedures and have considered the nature of these matters in our risk assessment and in determining the nature, timing, and extent of our procedures. This included performing procedures to understand the root cause disclosed by the CA, and if facts and circumstances noted in our examination agreed with what has been disclosed. We have also considered the procedures the CA has designed and noted if implemented properly and operated effectively, the controls would address the root cause. We did not perform any procedures subsequent to this report as to the effectiveness of the controls implemented.



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

KPMG

APPENDIX A

Detailing The Locations In-Scope

Location Name	Location Type	Location	In-Scope for Physical and Environmental Control Testing
Corporate Headquarters	RA Services	Tokyo, Japan	Yes
CA Office	RA Services	Tokyo, Japan	Yes
Offline key storage 1	Primary Data Center	Tokyo, Japan	Yes
Offline key storage 2	Backup/DR/Secondary Data Center	Osaka, Japan	Yes
Online CA hosting	Primary Data Center	Tokyo, Japan	Yes
Online CA hosting	Backup/DR/Secondary Data Center	Osaka, Japan	Yes
MPIC Servers	AWS Data Center 1	Asia Pacific (Tokyo)	No
MPIC Servers	AWS Data Center 2	Asia Pacific (Singapore)	No
MPIC Servers	AWS Data Center 3	US East (Ohio)	No
MPIC Servers	AWS Data Center 4	US West (Oregon)	No
MPIC Servers	AWS Data Center 5	Europe Central (Frankfurt)	No
MPIC Servers	AWS Data Center 6	Europe West (London)	No

KPMG

APPENDIX B

List of CAs in Scope

Root CAs
CA#1: Security Communication RootCA2
CA#2: Security Communication ECCRootCA1
CA#3: SECOM TLS RSA Root CA 2024
CA#4: SECOM TLS ECC Root CA 2024
OV TLS Issuing CAs
CA#5: SECOM Passport for Web SR 3.0 CA
CA#6: SECOM Passport for Web OV RSA CA 2024
CA#7: SECOM Passport for Web OV ECC CA 2024
CA#8: NII Open Domain CA - G7 RSA
CA#9: NII Open Domain CA - G8 RSA
CA#10: NII Open Domain CA - G7 ECC
EV TLS Issuing CAs
CA#11: SECOM Passport for Web EV 2.0 CA
CA#12: SECOM Passport for Web EV RSA CA 2024
CA#13: SECOM Passport for Web EV ECC CA 2024
Other CA
CA#14: FujiSSL Public Validation Authority - G3

KPMG

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 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
2	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	ECDSA Encryption	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 2.23.140.1.1
2	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	sha256WithECDSAEncryption	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 2.23.140.1.1
3	1	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	00EE8934D0CB80E0B2	rsaEncryption	4096bit	sha384WithRSAEncryption	Jan 31 05:11:55 2024 GMT	Jan 14 05:11:55 2049 GMT	2CEB72128E5877643515563501570 7A97D0D36E6	1435F225C5D252D7A21948CC3CE62AECFA88001E3DD72D1CC3555100EB372F93	2.23.140.1.1 2.23.140.1.2.1 2.23.140.1.2.2

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
3	2	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B1AD80E6588256D070530F78522D	rsaEncryption	4096bit	sha256WithRSAEncryption	Apr 9 05:28:15 2025 GMT	May 29 05:00:39 2029 GMT	2CEB72128E5877643515563501570 7A97D0D36E6	C8FB5BB81193CA9B531E2A0A568F14CC75D20924B98D2724DD243F63D813CF13	2.23.140.1.2.1 2.23.140.1.2.2 2.23.140.1.1
4	1	CN = SECOM TLS ECC Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM TLS ECC Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	00817A2CEF8F237A44	ECDSA Encryption	384bit	sha384WithECDSAEncryption	Jan 31 05:52:34 2024 GMT	Jan 14 05:52:34 2049 GMT	3B76117B2974E24E064C568240D0 212F7AB3C9D5	6AB2AB75F51CB4F4F0156203FBF6F646232F514BE059F62833308B82B4D72DB1	2.23.140.1.1 2.23.140.1.2.2
4	2	CN = SECOM TLS ECC Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	1DAFAA4C43ACB4320140CC9197BE2826	ECDSA Encryption	384bit	ecdsa-with-SHA384	Apr 9 06:34:14 2025 GMT	Jan 18 00:00:00 2038 GMT	3B76117B2974E24E064C568240D0 212F7AB3C9D5	22DA96F19EFC0429034A22755E9D7FE4746B3CAD56A013ED1C02F142A722B9A7	2.23.140.1.2.1 2.23.140.1.2.2 2.23.140.1.1
5	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	22B9B1AB809E203849C8A79FA9A4C417	rsaEncryption	2048bit	sha256WithRSAEncryption	Apr 9 05:08:22 2025 GMT	Mar 16 05:49:12 2028 GMT	CBEF3DEF8374A1A842F03B4036FA6D8294A92736	59F8A94C11BCD19FD4E0F1AC4D394E37913AE5FB5862A25A8ECD167BA3B9A3A2	2.23.140.1.2.2

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
5	2	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
6	1	CN = SECOM Passport for Web OV RSA CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	47A5911F0A7CBD021A9E99CFEA57A194	rsaEncryption	4096bit	sha384WithRSAEncryption	May 16 04:44:08 2024 GMT	Jan 12 00:00:00 2039 GMT	359BC579860B22F8F9E436B9E1F4287A578A8482	3520ABFC5A4C2558C89BF90EE29181D19518CCA6D0A57A6DC568F4F07C89F8DD	2.23.140.1.2.2
7	1	CN = SECOM Passport for Web OV ECC CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM TLS ECC Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	4FE6B3EF9CA8877E2819160426B614B4	ECDSAEncryption	384bit	sha384WithECDSAEncryption	May 16 05:26:53 2024 GMT	Jan 12 00:00:00 2039 GMT	F1C12480B407DBAEF95ECE1CF43307E3EDFFB7B8	42F56E96CD88B13C29258FCDC1213040ABF0C42EA29672991AEC3F3734CED056	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

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
9	1	CN = NII Open Domain CA - G8 RSA O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	47A591269A792F7FE456F83343A5ABD7	rsaEncryption	4096bit	sha384WithRSAEncryption	Aug 21 05:06:58 2025 GMT	Aug 21 00:00:00 2040 GMT	92AA38B1185A2B5C4BE7A10A40A5F24429D8C053	7A4AD9E1BA2DFB08F752A124032F7058868062E9841785623EB4136783A53FFC	2.23.140.1.2.2
10	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
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	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	1	CN = SECOM Passport for Web EV RSA CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	47A59120CF930432DF6E4126CCFFF684	rsaEncryption	4096bit	sha384WithRSAEncryption	May 16 05:01:37 2024 GMT	Jan 12 00:00:00 2039 GMT	BDAA9E649A3DF08AE1679CDF362A28197C7E7996	3E2464D4562FB4410F20C5C66C812C52BFBBEF31059CE55EF5BDB3703386AA74	2.23.140.1.1

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 Web EV ECC CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM TLS ECC Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	4FE6B3F069C4A8C79B6BE415245EB4EE	ECDSA Encryption	384bit	sha384WithECDSAEncryption	May 16 05:41:08 2024 GMT	Jan 12 00:00:00 2039 GMT	58BF80660FF03A4721291B47F324EA1AC7063BAE	0930324B3D817D306B6E01C6205B56A3AC856142FD5AAE166EF65160660DEE5C	2.23.140.1.1
14	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

KPMG

APPENDIX C

Certificate Policy/Certification Practice Statement

CA	Policy Name	Version	Date
CA#1 ～ CA#14	SECOM Publicly Trusted TLS Server Authentication Certificate Policy/Certification Practice Statement	1.01	February 12, 2026
	SECOM Publicly Trusted TLS Server Authentication Certificate Policy/Certification Practice Statement	1.00	October 22, 2025
CA#1 ～ CA#14	SECOM Publicly Trusted Certificate Policy/Certification Practice Statement	1.01	June 17, 2025
	SECOM Publicly Trusted Certificate Policy/Certification Practice Statement	1.00	May 26, 2025

APPENDIX D

#	Disclosure	Publicly Disclosed Link
1	SECOM: Invalid stateOrProvinceName	https://bugzilla.mozilla.org/show_bug.cgi?id=2004654

KPMG

APPENDIX E

#	Disclosure	Publicly Disclosed Link
1	SECOM: Non conformant SCT Encoding Due to SCT Modification by Cybertrust Japan (CTJ)	https://bugzilla.mozilla.org/show_bug.cgi?id=2007070
2	SECOM: Repository service disruption affecting subordinate CAs (CTJ)	https://bugzilla.mozilla.org/show_bug.cgi?id=2017840

STS MANAGEMENT'S ASSERTION

July 28, 2026

SECOM Trust Systems Co., Ltd. ("STS") operates the Certification Authority (CA) services for its CAs as enumerated in Appendix B and provides TLS CA services.

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

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

STS management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in providing its TLS CA services at its locations as detailed in Appendix A, throughout the period June 7, 2025 to June 6, 2026, STS has:

1. disclosed its TLS certificate lifecycle management business practices in its Certification Practice Statements and Certificate Policies enumerated in Appendix C, including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirements on the STS's website, and provided such services in accordance with its disclosed practices

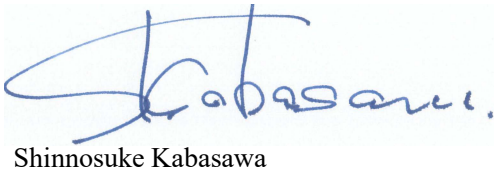
2. maintained effective controls to provide reasonable assurance that:
   - the integrity of keys and TLS certificates it manages is established and protected throughout their lifecycles; and
   - TLS subscriber information is properly authenticated (for the registration activities performed by STS)

3. 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 - TLS Baseline v2.9

STS has enumerated the information to Appendix D and Appendix E, 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 other matter described in Appendix E relates to a Bugzilla incident arising from the operation of an externally operated subordinate CA, which is outside the scope of Management's Assertion.

Appendix B, #14-1 CA did not issue certificates during the period June 7, 2025 to March 5, 2026 and was maintained online to provide revocation status information only. That CA was revoked on March 5, 2026.



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

APPENDIX A

Detailing The Locations In-Scope

Location Name	Location Type	Location	In-Scope for Physical and Environmental Control Testing
Corporate Headquarters	RA Services	Tokyo, Japan	Yes
CA Office	RA Services	Tokyo, Japan	Yes
Offline key storage 1	Primary Data Center	Tokyo, Japan	Yes
Offline key storage 2	Backup/DR/Secondary Data Center	Osaka, Japan	Yes
Online CA hosting	Primary Data Center	Tokyo, Japan	Yes
Online CA hosting	Backup/DR/Secondary Data Center	Osaka, Japan	Yes
MPIC Servers	AWS Data Center 1	Asia Pacific (Tokyo)	No
MPIC Servers	AWS Data Center 2	Asia Pacific (Singapore)	No
MPIC Servers	AWS Data Center 3	US East (Ohio)	No
MPIC Servers	AWS Data Center 4	US West (Oregon)	No
MPIC Servers	AWS Data Center 5	Europe Central (Frankfurt)	No
MPIC Servers	AWS Data Center 6	Europe West (London)	No

APPENDIX B

List of CAs in Scope

Root CAs
CA#1: Security Communication RootCA2
CA#2: Security Communication ECCRootCA1
CA#3: SECOM TLS RSA Root CA 2024
CA#4: SECOM TLS ECC Root CA 2024
OV TLS Issuing CAs
CA#5: SECOM Passport for Web SR 3.0 CA
CA#6: SECOM Passport for Web OV RSA CA 2024
CA#7: SECOM Passport for Web OV ECC CA 2024
CA#8: NII Open Domain CA - G7 RSA
CA#9: NII Open Domain CA - G8 RSA
CA#10: NII Open Domain CA - G7 ECC
EV TLS Issuing CAs
CA#11: SECOM Passport for Web EV 2.0 CA
CA#12: SECOM Passport for Web EV RSA CA 2024
CA#13: SECOM Passport for Web EV ECC CA 2024
Other CA
CA#14: 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 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
2	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	ECDSA Encryption	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 2.23.140.1.1
2	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	sha256WithECDSAEncryption	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 2.23.140.1.1
3	1	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	00EE8934D0CB80E0B2	rsaEncryption	4096bit	sha384WithRSAEncryption	Jan 31 05:11:55 2024 GMT	Jan 14 05:11:55 2049 GMT	2CEB72128E5877643515563501570 7A97D0D36E6	1435F225C5D252D7A21948CC3CE62AECFA88001E3DD72D1CC3555100EB372F93	2.23.140.1.1 2.23.140.1.2.1 2.23.140.1.2.2

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
3	2	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B1AD80E6588256D070530F78522D	rsaEncryption	4096bit	sha256WithRSAEncryption	Apr 9 05:28:15 2025 GMT	May 29 05:00:39 2029 GMT	2CEB72128E5877643515563501570 7A97D0D36E6	C8FB5BB81193CA9B531E2A0A568F14CC75D20924B98D2724DD243F63D813CF13	2.23.140.1.2.1 2.23.140.1.2.2 2.23.140.1.1
4	1	CN = SECOM TLS ECC Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM TLS ECC Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	00817A2CEF8F237A44	ECDSA Encryption	384bit	sha384WithECDSAEncryption	Jan 31 05:52:34 2024 GMT	Jan 14 05:52:34 2049 GMT	3B76117B2974E24E064C568240D0 212F7AB3C9D5	6AB2AB75F51CB4F4F0156203FBF6F646232F514BE059F62833308B82B4D72DB1	2.23.140.1.1 2.23.140.1.2.2
4	2	CN = SECOM TLS ECC Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	1DAFAA4C43ACB4320140CC9197BE2826	ECDSA Encryption	384bit	ecdsa-with-SHA384	Apr 9 06:34:14 2025 GMT	Jan 18 00:00:00 2038 GMT	3B76117B2974E24E064C568240D0 212F7AB3C9D5	22DA96F19EFC0429034A22755E9D7FE4746B3CAD56A013ED1C02F142A722B9A7	2.23.140.1.2.1 2.23.140.1.2.2 2.23.140.1.1
5	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	22B9B1AB809E203849C8A79FA9A4C417	rsaEncryption	2048bit	sha256WithRSAEncryption	Apr 9 05:08:22 2025 GMT	Mar 16 05:49:12 2028 GMT	CBEF3DEF8374A1A842F03B4036FA6D8294A92736	59F8A94C11BCD19FD4E0F1AC4D394E37913AE5FB5862A25A8ECD167BA3B9A3A2	2.23.140.1.2.2
5	2	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 #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
6	1	CN = SECOM Passport for Web OV RSA CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	47A5911F0A7CBD021A9E99CFEA57A194	rsaEncryption	4096bit	sha384WithRSAEncryption	May 16 04:44:08 2024 GMT	Jan 12 00:00:00 2039 GMT	359BC579860B22F8F9E436B9E1F4287A578A8482	3520ABFC5A4C2558C89BF90EE29181D19518CCA6D0A57A6DC568F4F07C89F8DD	2.23.140.1.2.2
7	1	CN = SECOM Passport for Web OV ECC CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM TLS ECC Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	4FE6B3EF9CA8877E2819160426B614B4	ECDSAEncryption	384bit	sha384WithECDSAEncryption	May 16 05:26:53 2024 GMT	Jan 12 00:00:00 2039 GMT	F1C12480B407DBAEF95ECE1CF43307E3EDFFB7B8	42F56E96CD88B13C29258FCDC1213040ABF0C42EA29672991AEC3F3734CED056	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 - G8 RSA O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	47A591269A792F7FE456F83343A5ABD7	rsaEncryption	4096bit	sha384WithRSAEncryption	Aug 21 05:06:58 2025 GMT	Aug 21 00:00:00 2040 GMT	92AA38B1185A2B5C4BE7A10A40A5F24429D8C053	7A4AD9E1BA2DFB08F752A124032F7058868062E9841785623EB4136783A53FFC	2.23.140.1.2.2
10	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

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
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	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	1	CN = SECOM Passport for Web EV RSA CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	47A59120CF930432DF6E4126CCFFF684	rsaEncryption	4096bit	sha384WithRSAEncryption	May 16 05:01:37 2024 GMT	Jan 12 00:00:00 2039 GMT	BDAA9E649A3DF08AE1679CDF362A28197C7E7996	3E2464D4562FB4410F20C5C66C812C52BFBBEF31059CE55EF5BDB3703386AA74	2.23.140.1.1
13	1	CN = SECOM Passport for Web EV ECC CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	CN = SECOM TLS ECC Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	4FE6B3F069C4A8C79B6BE415245EB4EE	ECDSAEncryption	384bit	sha384WithECDSAEncryption	May 16 05:41:08 2024 GMT	Jan 12 00:00:00 2039 GMT	58BF80660FF03A4721291B47F324EA1AC7063BAE	0930324B3D817D306B6E01C6205B56A3AC856142FD5AAE166EF65160660DEE5C	2.23.140.1.1
14	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

APPENDIX C

Certificate Policy/Certification Practice Statement

CA	Policy Name	Version	Date
CA#1 ～ CA#14	SECOM Publicly Trusted TLS Server Authentication Certificate Policy/Certification Practice Statement	1.01	February 12, 2026
	SECOM Publicly Trusted TLS Server Authentication Certificate Policy/Certification Practice Statement	1.00	October 22, 2025
CA#1 ～ CA#14	SECOM Publicly Trusted Certificate Policy/Certification Practice Statement	1.01	June 17, 2025
	SECOM Publicly Trusted Certificate Policy/Certification Practice Statement	1.00	May 26, 2025

APPENDIX D

#	Disclosure	Publicly Disclosed Link
1	SECOM: Invalid stateOrProvinceName	https://bugzilla.mozilla.org/show_bug.cgi?id=2004654

APPENDIX E

#	Disclosure	Publicly Disclosed Link
1	SECOM: Non conformant SCT Encoding Due to SCT Modification by Cybertrust Japan (CTJ)	https://bugzilla.mozilla.org/show_bug.cgi?id=2007070
2	SECOM: Repository service disruption affecting subordinate CAs (CTJ)	https://bugzilla.mozilla.org/show_bug.cgi?id=2017840