SUBSCRIBER AGREEMENT

Incorporating Time-Stamping Services Disclosure Statement

Version 1.5 | Effective Date: [29.6.2026] | Supersedes Version 1.4

NOTICE OF AMENDMENT

This Subscriber Agreement has been revised to incorporate a Time-Stamping Authority (TSA) Disclosure Statement as required under the MCMC Requirements for Certification Authorities to be Recognised as a Time Stamping Authority (TSA), specifically Clause 5.3 thereof. All other terms remain unchanged.

PLEASE READ THIS SUBSCRIBER AGREEMENT ("SUBSCRIBER AGREEMENT") BEFORE APPLYING FOR, ACCEPTING, OR USING A MSC TRUSTGATE.COM CERTIFICATE OR DIGITAL ID ("CERTIFICATE" OR "DIGITAL ID") OR TIME-STAMPING SERVICE ("TIME-STAMP SERVICE"). IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS SUBSCRIBER AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE THE CERTIFICATE OR TIME-STAMP SERVICE.

PART A — GENERAL TERMS AND CONDITIONS

1. Certificate Application and Description of Certificates

This Section details the terms and conditions regarding your application ("Certificate Application") for a Certificate and, if MSC Trustgate.com accepts your Certificate Application, the terms and conditions regarding the use of the Certificate to be issued by MSC Trustgate.com to you as "Subscriber" of that Certificate. A Certificate is a digitally signed message that contains a Subscriber's public key and associates it with information authenticated by MSC Trustgate.com or a MSC Trustgate.com-authorized entity. The Certificates provided under this Agreement are issued by MSC Trustgate.com. MSC Trustgate.com provides Certificates for both wired and wireless applications and under this Agreement offer three distinct assurances of certification services. Each level of Certificate provides specific functionality and security features and corresponds to a specific level of trust. You are responsible for choosing which Assurance Level of Certificate you need. For more detailed information about MSC Trustgate.com's certification services, please see the MSC Trustgate.com Certificate Policy / Certification Practice Statement ("CP/CPS") which may be accessed at https://www.msctrustgate.com.

(i) Low Assurance Certificates

It offers the lowest level of assurances. The Certificates are issued to individual Subscribers only, and authentication procedures are based on assurances that the Subscriber's distinguished name is unique and unambiguous within the domain of a particular Certification Authority ("CA") and that a certain e-mail address is associated with a public key. Low Assurance Certificates are appropriate for digital signatures, encryption, and access control for non-commercial or low-value transactions where proof of identity is unnecessary.

(ii) Medium Assurance Certificates

It offers a medium level of assurances. These Certificates are issued to individual Subscribers only. In addition to the Low-Level Assurance authentication procedures, Medium Assurance authentication includes procedures based on a comparison of information submitted by the certificate applicant against information in business records or databases or the database of a MSC Trustgate.com-approved identity proofing service. They can be used for digital signatures, encryption, and access control, including as proof of identity in medium-value transactions.

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

(iii) High Assurance Certificates

It provides the highest level of assurances which are issued to individuals and organizations for use with both client and server software. It may be used for digital signatures, encryption, and access control, including as proof of identity, in high-value transactions. Individual Certificates provide assurances of the identity of the Subscriber based on the personal (physical) presence of the Subscriber before a person that confirms the identity of the Subscriber using, at a minimum, a well-recognized form of government-issued identification and one other identification credential.

2. Processing Your Certificate Application

Upon MSC Trustgate.com's receipt of the necessary payment and upon completion of the authentication procedures required for the Certificate you have purchased, MSC Trustgate.com will process your Certificate Application. MSC Trustgate.com will notify you whether your Certificate Application is approved or rejected. If your Certificate Application is approved, MSC Trustgate.com will issue you a Certificate for your use in accordance with this Subscriber Agreement. Your use of the Personal Identification Number ("PIN") from MSC Trustgate.com to pick up the Certificate or otherwise installing or using the Certificate is considered your acceptance of the Certificate. After you pick up or otherwise install your Certificate, you must review the information in it before using it and promptly notify MSC Trustgate.com of any errors.

You also authorise MSC Trustgate.com to apply for a Legal Entity Identifier (LEI) on behalf through the RapidLEI platform where applicable. This authorization includes the right for MSC Trustgate.com to accept and agree to the applicable RapidLEI Terms of Service (https://rapidlei.com/documents/global-lei-system-terms/) and to carry out all actions necessary for the issuance, renewal, and management of the LEI.

You shall confirm that you have full legal authority to apply for LEI and to grant MSC Trustgate such authorization. Subscriber shall ensure that all information submitted for the purpose of LEI issuance or renewal is accurate and up-to-date and shall promptly notify MSC Trustgate.com of any changes to such information.

3. Obligations Upon Revocation or Expiration

Upon expiration or notice of revocation of your Certificate, you shall no longer use the Certificate for any purpose.

4. Ownership

Except as otherwise set forth herein, all right, title and interest in and to all, (i) registered and unregistered trademarks, service marks and logos; (ii) patents, patent applications, and patentable ideas, inventions, and/or improvements; (iii) trade secrets, proprietary information, and know-how; (iv) all divisions, continuations, reissues, renewals, and extensions thereof now existing or hereafter filed, issued, or acquired; (v) registered and unregistered copyrights including, without limitation, any forms, images, audiovisual displays, text, software; and (vi) all other intellectual property, proprietary rights or other rights related to intangible property which are used, developed, comprising, embodied in, or practiced in connection with any of the MSC Trustgate.com services identified herein ("MSC Trustgate.com Intellectual Property Rights") are owned by MSC Trustgate.com or its licensors, and you agree to make no claim of interest in or ownership of any such MSC Trustgate.com Intellectual Property Rights. You acknowledge that no title to the MSC Trustgate.com Intellectual Property Rights is transferred to you, and that you do not obtain any rights, express or implied, in the MSC Trustgate.com or its licensors' service, other than the rights expressly granted in this Subscriber Agreement. To the extent that you create any Derivative Work (any work that is based upon one or more preexisting versions of a work provided to you, such as an enhancement or modification, revision, translation, abridgement, condensation, expansion, collection, compilation or any other form in which such preexisting works may be recast, transformed or adapted) such Derivative Work shall be owned by MSC Trustgate.com or its licensors and all right, title and interest in and to each such Derivative Work shall automatically vest in MSC Trustgate.com or its licensors. MSC Trustgate.com shall have no obligation to grant you any right in any such Derivative Work. You may

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

not reverse engineer, disassemble or decompile the MSC Trustgate.com Intellectual Property or make any attempt to obtain source code to the MSC Trustgate.com Intellectual Property. You have the right to use the Certificate under the terms and conditions of this Subscriber Agreement.

5. Modifications to Agreement

Except as otherwise provided in this Subscriber Agreement, you agree, during the term of this Subscriber Agreement, that MSC Trustgate.com may: (i) revise the terms and conditions of this Subscriber Agreement; and/or (ii) change part of the services provided under this Subscriber Agreement at any time. Any such revision or change will be binding and effective thirty (30) days after posting of the revised Subscriber Agreement or change to the service(s) on MSC Trustgate.com's Web sites, or upon notification to you by e-mail or postal mail. You agree to periodically review MSC Trustgate.com's Web sites, including the current version of this Subscriber Agreement available on MSC Trustgate.com's Web sites, to be aware of any such revisions. If you do not agree with any revision to the Subscriber Agreement, you may terminate this Subscriber Agreement at any time by providing notice to MSC Trustgate.com. Notice of your termination will be effective on receipt and processing by MSC Trustgate.com. Any fees paid by you if you terminate this Subscriber Agreement are nonrefundable. By continuing to use MSC Trustgate.com services after any revision to this Subscriber Agreement or change in service(s), you agree to abide by and be bound by any such revisions or changes. MSC Trustgate.com is not bound by nor should you rely on any representation by (i) any agent, representative or employee of any third party that you may use to apply for MSC Trustgate.com's services; or in (ii) information posted on MSC Trustgate.com's Web site of a general informational nature. No employee, contractor, agent, or representative of MSC Trustgate.com is authorized to alter or amend the terms and conditions of this Subscriber Agreement.

6. Warranties

(i) MSC Trustgate.com Warranties

MSC Trustgate.com warrants to you that (i) there are no errors introduced by MSC Trustgate.com in your Certificate information as a result of MSC Trustgate.com's failure to use reasonable care in creating the Certificate; (ii) your Certificate complies in all material respects with the MSC Trustgate.com CP/CPS; and (iii) MSC Trustgate.com's revocation services and use of a repository conform to the MSC Trustgate.com CP/CPS in all material aspects. In respect of Time-Stamping Services, MSC Trustgate.com additionally warrants that each time-stamp token has been issued in conformance with the applicable time-stamp policy identified in Section 24 of this Agreement.

(ii) Your Warranty

You warrant to MSC Trustgate.com and anyone who relies on your Certificate that (i) all the information you provide to MSC Trustgate.com in your Certificate Application is accurate; (ii) no Certificate information you provided infringes the intellectual property rights of any third parties; (iii) the Certificate Application information has not been and will not be used for any unlawful purpose; (iv) you have been and will remain the only person possessing your private key and no unauthorized person has had or will have access to your private key; (v) you are using your Certificate exclusively for authorized and legal purposes consistent with this Subscriber Agreement; (vi) you are using your Certificate as an end-user Subscriber and not as a Certification Authority; and (vii) each digital signature created using your private key is your digital signature, and the Certificate has been accepted and is operational at the time the digital signature is created.

7. Disclaimers of Warranties

You agree that your use of MSC Trustgate.com's service(s) is solely at your own risk. All such services are provided on an "AS IS" and as available basis, except as otherwise noted in this Subscriber Agreement. MSC Trustgate.com expressly disclaims all warranties of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose and non-infringement. MSC Trustgate.com does not make any warranty that the

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

service will meet your requirements, or that the service will be uninterrupted, timely, secure or error free.

8. Indemnity

You agree to release, indemnify, defend and hold harmless MSC Trustgate.com and any of its contractors, agents, employees, officers, directors, shareholders, affiliates and assigns from all liabilities, claims, damages, costs and expenses, including reasonable attorney's fees and expenses, of third parties relating to or arising out of (i) this Subscriber Agreement or the breach of your warranties, representations and obligations under this Subscriber Agreement, (ii) falsehoods or misrepresentations of fact by you on the Certificate Application, (iii) any intellectual property or other proprietary right of any person or entity, (iv) failure to disclose a material fact on the Certificate Application if the misrepresentation or omission was made negligently or with intent to deceive any party, and (v) failure to protect the private key, or use a trustworthy system, or to take the precautions necessary to prevent the compromise, loss, disclosure, modification or unauthorized use of the private key under the terms of this Subscriber Agreement.

9. Limitations of Liability

This Section 9 applies to liability under contract (including breach of warranty), tort (including negligence and/or strict liability), and any other legal or equitable form of claim. If you initiate any claim, action, suit, arbitration, or other proceeding relating to services provided under this Subscriber Agreement, and to the extent permitted by applicable law, MSC Trustgate.com's total liability for damages sustained by you and any third party for any use or reliance on a Certificate or Time-Stamp Token shall be limited, in the aggregate, to the amounts set forth below.

The reliance limits below are as stated in the MSC Trustgate.com Certification Authority Disclosure Record maintained by MCMC pursuant to sub regulation 20(1) of the Digital Signature Regulations 1998. Subscribers are advised to refer to the Disclosure Record at https://www.mcmc.gov.my for the most up-to-date reliance limits.

Service / Product	**Reliance Limit (Liability Cap)**
AATL Individual Basic	Ringgit Malaysia Thirty Thousand (RM 30,000)
AATL Individual Pro	Ringgit Malaysia Forty Thousand (RM 40,000)
AATL Organization	Ringgit Malaysia Eighty Thousand (RM 80,000)
Document Signing (Medium Assurance)	Ringgit Malaysia Twenty-Five Thousand (RM 25,000)
Document Signing for Organization (Medium Assurance)	Ringgit Malaysia Fifty Thousand (RM 50,000)
Document Signing (High Assurance)	Ringgit Malaysia Four Hundred Thousand (RM 400,000)
MyDigital ID	Ringgit Malaysia Four Hundred Thousand (RM 400,000)
SSL Domain Validation (non-public trusted)	Ringgit Malaysia Five Hundred (RM 500)
SSL Organization Validation (non-public trusted)	Ringgit Malaysia Fifty Thousand (RM 50,000)

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

S/MIME Mailbox	Ringgit Malaysia Five Hundred (RM 500)
S/MIME Individual	Ringgit Malaysia Ten Thousand (RM 10,000)
S/MIME Sponsored / S/MIME Organization	As per CP/CPS and applicable service agreement

The liability limitations provided in this Section 9 shall be the same regardless of the number of digital signatures, transactions, or claims related to such certificate or time-stamp token. MSC Trustgate.com shall not be obligated to pay more than the total liability limitation for each certificate or time-stamp token. In no event shall MSC Trustgate.com be liable for any indirect, incidental, special, or consequential damages.

10. Fees, Payments, and Term of Service

As consideration for the Certificate, Time-Stamp Service, and associated services you have purchased, you agree to pay MSC Trustgate.com the applicable service(s) fees set forth on our Web site at the time of your selection, or, if applicable, upon receipt of your invoice from MSC Trustgate.com. All fees are due immediately. MSC Trustgate.com will provide you notice prior to the renewal of your services at least thirty (30) days in advance of the renewal date. All sums due and payable that remain unpaid after any applicable cure period will accrue interest as a late charge of one point five percent (1.5%) per month or the maximum amount allowed by law, whichever is less.

10A. Refund Policy

For Certificate services (Low, Medium and High Assurance): if a subscriber is not completely satisfied with a Certificate issued, the subscriber may request that MSC Trustgate.com revoke the Certificate within thirty (30) days of issuance and MSC Trustgate.com will provide the subscriber with a refund. Following the initial thirty (30) day period, a subscriber may request a refund if MSC Trustgate.com has breached a warranty or other material obligation under this Agreement or the CP/CPS.

For Time-Stamping Services: MSC Trustgate.com does not provide refunds for fees paid in respect of time-stamping services, including where time-stamp tokens have already been issued. This is consistent with the MSC Trustgate Time-Stamp Policy and Practice Statement (latest version of TSPPS, Annex B).

To request a refund for Certificate services, please contact: compliance@msctrustgate.com or via the contact methods specified on the MSC Trustgate.com website.

11. Force Majeure

Except for payment and indemnity obligations hereunder, neither party shall be deemed in default hereunder, nor shall it hold the other party responsible for, any cessation, interruption or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, act of God, war, armed conflict, terrorist action, labour strike, lockout, lockdown, boycott, or any other government restrictions, provided that the party relying upon this Section shall have given the other party written notice thereof promptly and, in any event, within five (5) days of discovery thereof and shall take all reasonable steps necessary under the circumstances to mitigate the effects of the force majeure event; provided further, that in the event a force majeure event extends for a period in excess of thirty (30) days in aggregate, the other party may immediately terminate this Subscriber Agreement.

12. Export

You acknowledge and agree that you shall not import, export, or re-export directly or indirectly, any commodity, including your Certificate or any Time-Stamp Token, to any country in violation of the laws and regulations of any applicable jurisdiction, including the export regulations of Malaysia.

13. Severability

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

You agree that the terms of this Subscriber Agreement are severable. If any term or provision is declared invalid or unenforceable, in whole or in part, that term or provision will not affect the remainder of this Subscriber Agreement; this Subscriber Agreement will be deemed amended to the extent necessary to make it enforceable, valid and, to the maximum extent possible consistent with applicable law, consistent with the original intentions of the parties.

14. Governing Law

You and MSC Trustgate.com agree that any disputes related to the services provided under this Subscriber Agreement shall be governed in all respects by and construed in accordance with the laws of Malaysia, excluding its conflict of laws rules. MSC Trustgate.com is obliged to adhere to applicable Malaysian legislation, including but not limited to:

- Digital Signature Act 1997 (Act 562), in particular Part VI (Section 70) relating to recognised date and time stamp services;
- Digital Signature Regulations 1998, Part IX (Regulations 58-70);
- Communications and Multimedia Act 1998;
- Personal Data Protection Act 2010 (Act 709); and
- MCMC Requirements for Certification Authorities (CA) to be Recognised as a Time Stamping Authority (TSA) (Effective 1 February 2018); and
- MCMC Certificate of Recognition for Date/Time Stamp Service No. PPTM-2/2024 (2) issued pursuant to Section 70 of the Digital Signature Act 1997, effective 25 July 2024, expiring 24 July 2027, subject to any regulations, guidelines, directives and administrative orders issued thereunder.

15. Complaints and Dispute Resolution

(i) Complaints Procedure

Any Subscriber wishing to raise a complaint regarding MSC Trustgate.com's services, including Certificate services or Time-Stamping Services, shall:

- Submit a written complaint to: compliance@msctrustgate.com (general) or digital-trust@msctrustgate.com (for Time-Stamping Services and digital trust matters) or in writing to MSC Trustgate.com Sdn. Bhd., Suite 2-9, Level 2, Block 4801 CBD Perdana, Jalan Perdana, 63000 Cyberjaya, Selangor, Malaysia;
- Include sufficient particulars identifying the subject matter of the complaint, the Certificate or time-stamp token concerned (if applicable), and the remedy sought; and
- MSC Trustgate.com shall acknowledge receipt of the complaint within five (5) business days and provide a substantive response within thirty (30) days.

(ii) Dispute Resolution

Prior to pursuing any formal legal or dispute resolution mechanism, all parties shall provide written notice of a dispute to MSC Trustgate.com and attempt to resolve the matter directly through good faith negotiations for a period of at least sixty (60) days from the date of the notice. Nothing in this Section will be deemed as preventing either party from seeking injunctive relief (or any other provisional remedy) from any Malaysian court having jurisdiction as is necessary to protect either party's name, proprietary information, trade secret, know-how, or any other intellectual property rights.

If a dispute is not resolved through negotiation:

- For claimants who are residents of Malaysia: the dispute shall be submitted to the courts of Malaysia.

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

- For all other claimants: the dispute shall be resolved by arbitration administered by the Asian International Arbitration Centre (AIAC) in Kuala Lumpur, in accordance with the Rules of AIAC.

16. Non-Assignment

Except as otherwise set forth herein, your rights under this Agreement are not assignable or transferable. Any attempt by your creditors to obtain an interest in your rights under this Subscriber Agreement, whether by attachment, levy, garnishment or otherwise, renders this Subscriber Agreement voidable at MSC Trustgate.com's option.

17. Notices

You will make all notices, demands or requests to MSC Trustgate.com with respect to this Subscriber Agreement in writing to: MSC Trustgate.com Sdn. Bhd., Suite 2-9, Level 2, Block 4801 CBD Perdana, Jalan Perdana, 63000 Cyberjaya, Selangor, Malaysia. For matters relating to Time-Stamping Services, notices may also be directed to: digital-trust@msctrustgate.com (Attention: Digital Trust & Governance Manager), Tel: +603 8318 1800.

18. Survival

This Subscriber Agreement shall be applicable for as long as the Certificate remains valid, and you have not breached any provision of this Subscriber Agreement. The indemnity obligations under Section 8, the limitations of liability under Section 9, and the relying party obligations under Section 27 shall survive the termination or expiration of this Agreement.

19. Privacy

You agree that MSC Trustgate.com may place in your Certificate certain information that you provide for inclusion in your Certificate. You also agree that MSC Trustgate.com may publish your Certificate and information about its status in MSC Trustgate.com's repository of Certificate information and make this information available to other repositories. MSC Trustgate.com is a registered party with the Jabatan Perlindungan Data Peribadi (JPDP) and complies with the Personal Data Protection Act 2010 (Act 709). MSC Trustgate.com's privacy policy is available at https://www.msctrustgate.com/repository.

20. Fiduciary Duty of Private Key

When Trustgate holds the private key corresponding to a public key listed in a certificate which it has issued, Trustgate shall hold the private key as a fiduciary of the subscriber named in the certificate and may use that private key which subscriber hereby grants their permission for the said usage.

21. Entire Agreement

This Subscriber Agreement, together with the MSC Trustgate.com CP/CPS and the Time-Stamping Services Disclosure Statement set out in Sections 24 to 31 herein, constitutes the entire understanding and agreement between MSC Trustgate.com and you with respect to the transactions contemplated, and supersedes any and all prior or contemporaneous oral or written representation, understanding, agreement or communication concerning the subject matter hereof. Section headings are inserted for convenience of reference only.

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

PART B — TIME-STAMPING SERVICES TERMS AND TSA DISCLOSURE STATEMENT

Sections 22-31 constitute the TSA Disclosure Statement as required under Clause 5.3 of the MCMC Requirements for Certification Authorities (CA) to be Recognised as a Time Stamping Authority (TSA).

These sections are incorporated into and form part of this Subscriber Agreement. References to "you" and "Subscriber" in this Part B apply equally to Relying Parties where the context so requires.

22. Time-Stamping Authority — Identification and Contact Information

MSC Trustgate.com Sdn. Bhd. (Company No. 199901003331) is licensed by the Malaysian Communications and Multimedia Commission (MCMC) as a Certification Authority (CA) and is recognised by MCMC as a Time Stamping Authority (TSA) pursuant to the Digital Signature Act 1997 (Part VI, Section 70) and the Digital Signature Regulations 1998 (Part IX, Regulations 58-70).

Detail	**Information**
TSA Name	MSC Trustgate.com Sdn. Bhd.
Registered Address	Suite 2-9, Level 2, Block 4801 CBD Perdana, Jalan Perdana, 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia
Tel	+603 8318 1800
Fax	+603 8319 1800
Email	digital-trust@msctrustgate.com (TSA / Digital Trust enquiries); compliance@msctrustgate.com (general)
Website / Repository	https://www.msctrustgate.com / https://www.msctrustgate.com/repository
MCMC Certificate of Recognition No.	PPTM-2/2024 (2) (Valid: 25 July 2024 - 24 July 2027)

23. TSA Conformance, Recognition, and Audit

MSC Trustgate.com's conformance with the MCMC TSA Requirements and the applicable audit arrangements are as set out in the MSC Trustgate Time-Stamp Policy and Practice Statement (TSPPS) at Section 5.1.4 (Conformance) and Section 5.6.10 (Compliance), and in the TSA Disclosure Statement at Annex B, read together with the MSC Trustgate CP/CPS. These documents are available at https://www.msctrustgate.com/repository.

24. Time-Stamp Policy and Technical Specifications

MSC Trustgate.com's Time-Stamping Services operate pursuant to the MSC Trustgate Time-Stamp Policy and Practice Statement (TSPPS), available at https://www.msctrustgate.com/repository. The applicable time-stamp policy, technical specifications and policy parameters are as set out in the TSPPS, in particular:

- the time-stamp policy and its object identifier (OID): Section 5.1.2 (Identification);
- the hash and signature algorithms supported for time-stamping: Annex A.4 (Algorithms for Time Stamping);
- the accuracy of the time in time-stamp tokens with respect to Malaysia Standard Time (MST) and clock synchronisation: Section 5.5.3 (Clock Synchronization with MST); and
- the expected life-time of the signature used to sign the time-stamp token: the TSA Disclosure Statement at Annex B.

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

The complete TSA Practice Statement is incorporated within the MSC Trustgate CP/CPS, available at the same repository. The TSPPS and this TSA Disclosure Statement together constitute the governing documents for the time-stamping service.

25. Limitations on Use of the Time-Stamping Service

MSC Trustgate.com's Time-Stamping Service is intended for use in applications requiring cryptographically verifiable proof that a datum existed at a particular point in time. The following limitations apply:

- Time-stamp tokens must not be relied upon beyond the expiry of the TSU signing key usage period without applying additional time-stamps or archiving procedures as described in RFC 3161 / Annex D of the MCMC TSA Requirements.
- The Time-Stamping Service shall be used only for lawful purposes consistent with Malaysian law and the terms of this Agreement.
- MSC Trustgate.com reserves the right to suspend the Time-Stamping Service in the event of a detected clock desynchronisation, TSU key compromise, or force majeure event, without liability to subscribers or relying parties.
- The time-stamp token confers no right to continued access to the service beyond the subscription period.

26. Subscriber Obligations — Time-Stamping Services

In addition to the general warranties and obligations in Section 6 of this Agreement, you as Subscriber of the Time-Stamping Service specifically acknowledge and undertake the following:

- Upon obtaining a time-stamp token, you should verify that the time-stamp token has been correctly signed and that the private key used to sign the time-stamp token has not been compromised. The TSU's certificate status may be checked via MSC Trustgate.com's CRL or OCSP services at https://www.msctrustgate.com/repository.
- You acknowledge that the evidential value of a time-stamp token may be diminished if you fail to take appropriate steps to preserve the time-stamp token and the integrity of the time-stamped datum.
- You must not submit false, misleading, or unlawful data for time-stamping.
- You are solely responsible for ensuring long-term verification of time-stamp tokens by applying additional timestamps before the expiry of the original TSU signing key or the cryptographic algorithm's security period, in accordance with Annex D of the MCMC TSA Requirements.

27. Relying Party Obligations

Any party who relies on a time-stamp token issued by MSC Trustgate.com ("Relying Party") shall, as a condition of such reliance, comply with the following obligations:

- Verify that the time-stamp token has been correctly signed and that the private key used to sign the time-stamp token has not been compromised up to the time of verification. This verification must include a check of the current revocation status of the TSU's certificate via MSC Trustgate.com's CRL or OCSP services at https://www.msctrustgate.com/repository. During the TSU certificate validity period, the CRL or OCSP response provides the current revocation status. If the time of verification exceeds the end of the TSU certificate validity period, the Relying Party should consult the archive of revocation status information or apply an additional time-stamp as described in Annex D of the MCMC TSA Requirements.
- Take into account any limitations on the usage of the time-stamp token as stated in the applicable time-stamp policy and as identified in Section 25 of this Agreement.
- After expiry of the TSU certificate, the Relying Party shall: (i) verify that the TSU private key has not been revoked; and (ii) verify that the cryptographic hash function and the signing algorithm

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

used in the time-stamp token are still considered cryptographically secure. Where either condition is not satisfied, the time-stamp token should not be relied upon without applying additional protective measures such as a further time-stamp from MSC Trustgate.com.

- Take into account any other precautions prescribed in this Agreement, the CP/CPS, or any applicable written law in Malaysia.
- The Relying Party acknowledges that they have sufficient information to make an informed decision as to the extent to which they choose to rely on a time-stamp token, and that they are solely responsible for deciding whether or not to rely on such information.
- Relying Parties shall indemnify MSC Trustgate.com for any claims, damages, or losses arising from: (i) the Relying Party's failure to perform the obligations stated in this Section; (ii) the Relying Party's reliance on a time-stamp token that is not reasonable under the circumstances; or (iii) the Relying Party's failure to check the revocation status of the TSU certificate.

28. How to Verify a Time-Stamp Token

To "reasonably rely" on a time-stamp token issued by MSC Trustgate.com, a Relying Party should perform the following verification steps:

Step	Action	Detail
1	Obtain TSU Certificate	Obtain the TSU's signing certificate from the time-stamp or from MSC Trustgate.com's repository at https://www.msctrustgate.com/repository.
2	Validate Certificate Chain	Verify that the TSU certificate chains up to the MSC Trustgate.com Root CA and that all certificates in the chain are valid at the time the time-stamp was issued.
3	Check Revocation Status	Check the revocation status of the TSU certificate using CRL or OCSP. CRL Distribution Points and OCSP URLs are embedded in the TSU certificate. Revocation information for Timestamp Certificates is retained for at least 10 years after certificate expiry.
4	Verify Token Signature	Verify the cryptographic signature of the time-stamp token using the TSU's public key. Confirm that the hash value in the token matches the hash of the datum that was time-stamped.
5	Confirm Accuracy	Confirm that the time in the time-stamp token is within ±1 second of MST and that the accuracy field in the token is consistent with the declared accuracy in Section 24.
6	Long-term Verification	For verification beyond the TSU certificate validity period, apply an additional time-stamp from MSC Trustgate.com to protect the integrity of the original token, or store the time-stamped data in a secure archive. Refer to Annex D of the MCMC TSA Requirements for further guidance.

29. TSA Event Log Retention

MSC Trustgate.com maintains and retains event logs in connection with its Time-Stamping Services in accordance with the TSPPS at Section 5.6.11 (Collection of Evidence), read together with the MSC Trustgate CP/CPS at Section 5.4.3 (retention period for audit log) and Sections 5.4 (Audit Logging Procedures) and 5.5 (Records Archival). The retention period for TSA event logs is as stated in those provisions.

30. TSA Termination Provisions

In the event that MSC Trustgate.com decides to cease or terminate its Time-Stamping Services, MSC Trustgate.com shall execute the following minimum procedures to protect the interests of Subscribers and Relying Parties:

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

- **Advance Notice:** MSC Trustgate.com shall provide advance notice of termination to all Subscribers and Relying Parties via the MSC Trustgate.com website and direct communication, with reasonable advance notice to allow Subscribers to migrate to an alternative TSA service.
- **Archive Transfer:** MSC Trustgate.com shall transfer obligations for maintaining event log and audit archives (as described in Section 29) to another licensed certification authority appointed by the MCMC, to ensure the continued availability of records necessary to verify the correctness of previously issued time-stamp tokens.
- **Public Key / Certificate Availability:** MSC Trustgate.com shall maintain or transfer to another licensed certification authority appointed by the MCMC its obligations to make available its TSU public keys and certificates to Relying Parties for a reasonable period (minimum of 10 years after the last issued time-stamp token's expiry).
- **TSU Private Key Destruction:** TSU private keys, including all backup copies, shall be destroyed in a secure manner such that the private keys cannot be retrieved.
- **TSU Certificate Revocation:** MSC Trustgate.com shall take steps to have the TSU's certificates revoked upon cessation of the Time-Stamping Service.
- **Termination of Subcontractor Authorisations:** MSC Trustgate.com shall terminate the authorisation of all subcontractors acting on its behalf in relation to the issuance of time-stamp tokens, effective from the date of cessation of the Time-Stamping Service, consistent with Section 5.5.4(b) of the MCMC TSA Requirements.
- **Cost Coverage:** MSC Trustgate.com maintains an arrangement to cover the costs of fulfilling these minimum termination requirements, including in circumstances where MSC Trustgate.com faces financial difficulty.

The termination provisions in this Section shall survive the expiry or termination of this Subscriber Agreement and shall remain binding on MSC Trustgate.com.

31. Applicable Agreements, Practice Statement, and Related Documents

The following documents govern the Time-Stamping Services provided by MSC Trustgate.com and are made available to Subscribers and Relying Parties:

Document	Access
MSC Trustgate.com CP/CPS (incorporating TSA Practice Statement)	https://www.msctrustgate.com/repository
This Subscriber Agreement (incorporating TSA Disclosure Statement)	https://www.msctrustgate.com
MCMC TSA Requirements	https://www.mcmc.gov.my
Digital Signature Act 1997 (Act 562)	https://www.agc.gov.my
Digital Signature Regulations 1998	https://www.agc.gov.my
MSC Trustgate.com Privacy Policy	https://www.msctrustgate.com/repository

These documents are available at no charge. Any material amendments to the CP/CPS or this Subscriber Agreement will be notified to Subscribers in accordance with Section 5 of this Agreement.

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

SCHEDULES

This Agreement incorporates the following Schedules and the Common SLA. Each Schedule forms an integral part of this Subscriber Agreement.

Schedule	Title	Subject Matter
Schedule A	TSA Disclosure Statement Compliance Map	Regulatory mapping of the 14 mandatory disclosure items under Clause 5.3 of the MCMC TSA Requirements
Schedule B	Document Signing (AATL & Non-AATL)	Issuance and use of document-signing Certificates
Schedule C	Cloud Signing (CSC API, MyTrust365, Key Custody)	Cloud-based / remote digital signing
Schedule D	Hardware-Based Signing (USB Tokens & HSMs)	Local key generation and storage
Schedule E	S/MIME (Secure Email Certificates)	Email signing and encryption certificates
Schedule F	TLS/SSL (Server Certificates)	DV/OV/EV server certificates
Common SLA	Availability, Support & Credits	Service levels applicable across all Schedules

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

SCHEDULE A — TSA DISCLOSURE STATEMENT COMPLIANCE MAP

This schedule maps each of the 14 mandatory disclosure items under Clause 5.3 of the MCMC TSA Requirements to the relevant section of this Subscriber Agreement, for audit and regulatory reference purposes.

Ref	Clause 5.3 Requirement	Agreement Section	Status / Note
5.3(a)	TSA contact information	Sections 17 & 22	COVERED — Name, address, email, tel provided
5.3(b)	Time-stamp policy being applied (OID)	Section 24	COVERED — CP/CPS OID 1.3.6.1.4.1.49530.1.3.1;
5.3(c)	At least one hash algorithm for time-stamping	Section 24	COVERED — SHA-256 (OID: 2.16.840.1.101.3.4.2.1) minimum; SHA-384/512 also supported
5.3(d)	Expected life-time of TSA signing signature	Section 24	COVERED — Expected lifetime of signing signature: 5 years (TSPPS v1.5 Annex B). TSU key rotation: max 455 days. TSU Certificate: max 4,105 days.
5.3(e)	Accuracy of time in tokens with respect to MST	Section 24	COVERED — Within ±1 second of MST (NMIM); confirmed annually by NMIM
5.3(f)	Limitations on use of the time-stamping service	Section 25	COVERED — Six specific usage limitations stated
5.3(g)	Subscriber's obligations (per clause 5.4.3)	Section 26	COVERED — Six specific TSA subscriber obligations including token verification duty
5.3(h)	Relying party's obligations (per clause 5.4.4)	Section 27	COVERED — Four specific relying party obligations; indemnity provision included
5.3(i)	How to verify time-stamp token / reasonable reliance	Section 28	COVERED — Six-step verification guide; revocation check procedure; long-term verification noted
5.3(j)	Period TSA event logs are retained	Section 29	COVERED — 10 years for audit logs, CRL entries, OCSP responses, archive records (from CP/CPS s.5.4.3, 4.9.8)
5.3(k)	Applicable legal system including compliance with national law on time-stamping	Section 14	COVERED — DSA 1997 s.70; DSR 1998 Reg. 58-70; CMA 1998; PDPA 2010 all expressly referenced
5.3(l)	Limitations of liability	Section 9	COVERED — Liability caps updated to match MCMC Disclosure Record (DR Ref: LPBP-2/2025 (5)) per DR Section 12 reliance limits.

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

5.3(m)	Procedures for complaints and dispute settlement	Section 15	COVERED — Complaints procedure (5-day acknowledgement, 30-day response); 60-day good faith negotiation; AIAC arbitration for non-Malaysian claimants
5.3(n)	Whether TSA has been assessed as conformant and by which body	Section 23	COVERED — WebTrust auditor; MCMC recognition; annual reporting to MCMC.

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

SCHEDULE B — DOCUMENT SIGNING (AATL & NON-AATL)

B1. Scope and Application

This Schedule governs the issuance, management, and use of document-signing Certificates issued by MSC Trustgate.com Sdn. Bhd. ("MSC Trustgate.com") to Subscribers for the purpose of applying legally binding digital signatures to electronic documents, including but not limited to Portable Document Format (PDF) files and Office Open XML (OOXML) formats. This Schedule applies to both Adobe Approved Trust List (AATL) Certificates and non-AATL document-signing Certificates issued under MSC Trustgate.com's Certificate Policy and Certification Practice Statement (CP/CPS).

This Schedule is to be read in conjunction with the general terms of the Subscriber Agreement. In the event of any inconsistency between this Schedule and the general terms, this Schedule shall prevail in respect of the subject matter hereof.

B2. Certificate Classes and Identity Assurance

Document-signing Certificates are issued at the following assurance levels, corresponding to the general definitions in Part A of this Agreement:

(a) Medium Assurance (Class 2). Document-signing Certificates issued in accordance with the Digital Signature Act 1997 (Act 562) and the Digital Signature Regulations 1998 at Class 2 Level of Assurance. Issued to individuals or organisations following identity verification against a Reliable Data Source as specified in MSC Trustgate.com's CP/CPS. The Certificate shall contain the Subscriber's authenticated name (commonName), national identifier such as MyKad or Passport number (serialNumber), and country code (countryName). Products in this class include Digital Signing (Basic), Digital Signing (Pro), and Digital Signing (Organisation). The applicable liability limit for this class is set out in Section 9 of the Agreement.

(b) High Assurance (Class 3). Document-signing Certificates issued at Class 3 Level of Assurance under the Digital Signature Act 1997 (Act 562). Issued to individuals whose identity has been certified by a notary public duly appointed under the Notaries Public Act 1959, in addition to standard identity verification requirements under MSC Trustgate.com's CP/CPS. Suitable for high-value or legally significant transactions where enhanced identity assurance is required. The applicable liability limit for this class is set out in Section 9 of the Agreement.

B3. Subscriber Obligations

Subscriber shall use the document-signing Certificate solely for its intended purpose, protect the associated private key from unauthorised access or disclosure, and notify MSC Trustgate.com without undue delay upon loss, compromise, or any change in the particulars represented in the Certificate.

B4. Certificate Content and Profiles

All document-signing Certificates issued under this Schedule will contain:

(a) The Subscriber's authenticated subject attributes (name, organisation where applicable, email address) as verified by MSC Trustgate.com or the RA;

(b) Key usage extensions set to at minimum **digitalSignature** and **nonRepudiation** (also referred to as **contentCommitment**);

(c) Extended key usage extensions appropriate to the Certificate profile as defined in MSC Trustgate.com's CP/CPS;

(d) Certificate validity periods as specified in MSC Trustgate.com's CP/CPS for the relevant Certificate class;

(e) AATL programme-specific OIDs where the Certificate is issued under the AATL programme; and

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

(f) CRL Distribution Points and/or OCSP URLs to enable relying parties to check the revocation status of the Certificate; and

(g) Key pairs generated using a minimum of RSA 2048-bit or Elliptic Curve 256-bit, signed with SHA-256 or stronger hash algorithms, consistent with MSC Trustgate.com's CP/CPS and applicable AATL programme requirements. MSC Trustgate.com reserves the right to require stronger algorithms as cryptographic standards evolve and shall provide Subscribers with reasonable advance notice of any mandatory algorithm upgrade.

B5. Permitted and Prohibited Uses

(a) Permitted Uses. Document-signing Certificates issued under this Schedule may be used for:

- Applying digital signatures to electronic documents in PDF, OOXML, or other formats supported by MSC Trustgate.com's Certificate profile;
- Applying certification signatures to PDF documents (author signatures) where the Subscriber is the document creator;
- Enabling Long-Term Validation (LTV) of signed documents in conjunction with a trusted time-stamp; and
- Any other purpose expressly authorised in writing by MSC Trustgate.com.

(b) Prohibited Uses. Document-signing Certificates issued under this Schedule shall not be used for:

- Code signing, or software distribution signing;
- TLS/SSL server authentication;
- Client authentication as a standalone identity credential, unless expressly authorised;
- Signing of documents or transactions on behalf of a third party without that party's knowledge and consent;
- Any purpose that violates applicable Malaysian law or MSC Trustgate.com's CP/CPS; or
- Any purpose that misrepresents the nature, scope, or legal effect of the digital signature to a Relying Party.

B6. Key Management — Local and Hosted Keys

(a) Locally Stored Keys. Where Subscriber generates and stores the private key on a local device or hardware token:

- The device or token must meet the minimum security requirements specified in Schedule D (Hardware-Based Signing);
- Subscriber must set a unique Personal Identification Number (PIN) or activation data upon first use and must not share this with any other person;
- The token must be configured to enforce PIN lockout after a maximum of five (5) consecutive incorrect entries;
- Subscriber must store the physical token securely when not in use and must immediately notify MSC Trustgate.com upon loss, theft, or suspected compromise.

(b) Hosted Keys (Cloud Signing). Where the private key is generated and held by MSC Trustgate.com or its authorised Remote Signing Service MSC Trustgate.com (RSSP), the terms of Schedule C shall apply. Subscriber's authorisation of key custody is governed by Schedule C, Clause C2.

(c) Key Backup. Key backup is only permitted to the extent expressly permitted by MSC Trustgate.com's CP/CPS for the relevant Certificate class. Subscriber must not export or duplicate a private key in a manner not authorised by MSC Trustgate.com.

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

B7. Long-Term Validation (LTV) and Archival

(a) Subscriber acknowledges that the long-term validity of a document-signing Certificate depends on more than the Certificate's own validity period. To ensure that signed documents remain verifiable after the Certificate expires or is revoked, Subscriber should:

- Apply a trusted time-stamp from a recognised Time Stamping Authority (TSA), including MSC Trustgate.com's own TSA service, at the time of signing or immediately thereafter;
- Embed within the signed document all relevant Certificate chain, CRL, and/or OCSP response data at the time of signing to enable LTV; and
- Preserve the signed document and its associated validation evidence in a manner that prevents undetected alteration.

(b) MSC Trustgate.com recommends that Subscribers and Relying Parties apply additional time-stamps before the expiry of the original signing certificate's validity or the security period of the cryptographic algorithms used, in order to extend the verifiable life of the signed document.

(c) MSC Trustgate.com shall retain CRL and OCSP information for a period of not less than ten (10) years after Certificate expiry to support long-term verification of documents signed under this Schedule.

(d) Subscriber acknowledges that where AATL Certificates are used in long-term archival scenarios, the evidential value of a digitally signed document depends on the availability of MSC Trustgate.com's revocation information beyond the Certificate's validity period. MSC Trustgate.com's retention obligations under this clause are designed to support this requirement.

B8. Revocation and Certificate Status

(a) Subscriber must request revocation of the document-signing Certificate from MSC Trustgate.com without undue delay upon the occurrence of any of the following:

- Loss, theft, or suspected compromise of the private key or the hardware token on which it is stored;
- Discovery of any inaccuracy in the Certificate information;
- Change in the Subscriber's legal name, organisational affiliation, or other material information represented in the Certificate; or
- Termination of the Subscriber's authority to sign on behalf of any organisation named in the Certificate.

(b) Revocation requests shall be submitted to MSC Trustgate.com at validation@msctrustgate.com or through MSC Trustgate.com's online revocation interface at https://www.msctrustgate.com.

(c) MSC Trustgate.com shall publish revocation status via CRL and/or OCSP in accordance with MSC Trustgate.com's CP/CPS. The time between receipt of a valid revocation request and its publication in a CRL or OCSP response shall not exceed the maximum revocation publication delay stated in MSC Trustgate.com's CP/CPS.

(d) Subscriber acknowledges that MSC Trustgate.com may also revoke a Certificate without the Subscriber's request where required by law, by applicable programme rules (including AATL programme requirements), or where MSC Trustgate.com becomes aware of circumstances that make revocation necessary to protect the integrity of MSC Trustgate.com's PKI hierarchy.

B9. Reliance and Monetary Limits

(a) Relying Parties who rely on a document-signing Certificate issued under this Schedule should, before such reliance, validate the Certificate status using the CRL or OCSP service referenced in the Certificate and verify the digital signature mathematically.

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

(b) The maximum Reliance Limits applicable to document-signing Certificates are as set out in Section 9 of the Agreement and the MCMC Certification Authority Disclosure Record referenced therein. For convenience:

Certificate Class	**Reliance Limit**
AATL Individual Basic	RM 30,000
AATL Individual Pro	RM 40,000
AATL Organization	RM 80,000
Document Signing (Medium Assurance)	RM 25,000
Document Signing for Organisation (Medium Assurance)	RM 50,000
Document Signing (High Assurance)	RM 400,000

(c) Where a Relying Party fails to perform the verification steps in clause B9(a) prior to reliance, MSC Trustgate.com shall not be liable for losses arising from that reliance beyond the limits stated above, and the Relying Party's own contributory failure shall be taken into account in any assessment of liability.

(d) The reliance limits in this clause are per-Certificate limits and apply in aggregate across all transactions and claims associated with that Certificate, consistent with Section 9 of the Agreement.

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

SCHEDULE C — CLOUD SIGNING (CSC API, MYTRUST365, AUTHORIZATION OF KEY CUSTODY)

C1. Scope and Application

This Schedule governs the provision and use of cloud-based digital signature services operated by MSC Trustgate.com or its authorised Remote Signing Service MSC Trustgate.com (RSSP), including services exposed through the Cloud Signature Consortium (CSC) API standard and MSC Trustgate.com's proprietary MyTrust365 platform. It applies to all Subscribers who elect to use remote or cloud-based signing as an alternative to local key storage.

Under cloud signing, the Subscriber's private signing key is generated within, and signing operations are performed by, MSC Trustgate.com's or the RSSP's Signature Activation Module (SAM) and Hardware Security Module (HSM) infrastructure, rather than on a device controlled by the Subscriber.

C2. Authorization of Key Custody and Signing Operations

By enrolling for cloud signing services, Subscriber expressly and irrevocably authorises MSC Trustgate.com and/or its RSSP to:

(a) Generate the Subscriber's private key pair within certified HSM infrastructure maintained by MSC Trustgate.com, under dual-person control and in compliance with MSC Trustgate.com's CP/CPS;

(b) Hold and protect the private key within the HSM for the duration of the Certificate validity period, subject to the security controls set out in this Schedule;

(c) Perform digital signing operations using the Subscriber's private key solely upon: - Receipt of a valid authentication and authorisation from the Subscriber through the multi-factor authentication (MFA) mechanism described in Clause C4; and - A per-transaction or per-session signing request that is cryptographically bound to the document or data to be signed, ensuring that the signing key cannot be used outside the authorised transaction;

(d) Destroy all copies of the private key upon the earlier of: (i) revocation of the Certificate; (ii) expiry of the Certificate and completion of any applicable retention period; or (iii) termination of the Subscriber's cloud signing subscription, in each case in accordance with MSC Trustgate.com's documented key destruction procedures.

Subscriber acknowledges that this authorisation is a prerequisite for the provision of cloud signing services and that the Subscriber's digital signature applied via cloud signing carries the same legal effect as a signature applied using a locally stored private key.

C3. Fiduciary Duty and Sole Signing Obligation

(a) Where MSC Trustgate.com holds a Subscriber's private key, MSC Trustgate.com holds that key as a fiduciary of the Subscriber. MSC Trustgate.com shall not use the Subscriber's private key for any purpose other than performing digital signing operations at the Subscriber's express direction.

(b) MSC Trustgate.com warrants that it has implemented organisational and technical controls to ensure that no single individual within MSC Trustgate.com can unilaterally access or use a Subscriber's private key.

(c) Subscriber remains solely responsible for the digital signatures applied using their credentials. MSC Trustgate.com's role in executing the signing operation does not transfer or diminish the Subscriber's legal responsibility for the content of signed documents or the representations made by those signatures.

C4. Authentication, Authorization, and Sole Control

(a) Multi-Factor Authentication (MFA). Before any signing operation may be performed, Subscriber must authenticate to the cloud signing platform using at least two independent factors,

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

such as: - A knowledge factor (password or PIN); - A possession factor (one-time password via registered mobile device, hardware OTP token, or push notification to a registered authenticator application); or - An inherence factor (biometric verification) where supported.

(b) Audit Logging. MSC Trustgate.com shall maintain comprehensive audit logs of all authentication events, authorisation requests, and signing operations performed under each Subscriber's account.

(b) Sole Control. MSC Trustgate.com's authentication and authorisation mechanisms are designed to ensure that only the Subscriber can initiate signing operations and that MSC Trustgate.com cannot perform signing on behalf of the Subscriber without the Subscriber's active involvement. Subscriber must not share authentication credentials or attempt to delegate signing authority in a manner that undermines sole control.

C5. API Terms and Integration Requirements

(a) Subscriber and any authorised integration partner shall keep all API credentials (client identifiers, secrets, access tokens, and API keys) confidential and shall not disclose them to any third party.

(b) Subscriber shall implement rate limiting and abuse prevention controls in any application integrating with the CSC API or MyTrust365 platform, consistent with limits published by MSC Trustgate.com from time to time.

(c) MSC Trustgate.com shall provide Subscribers with reasonable advance notice of any planned changes to API versions, endpoints, or authentication mechanisms that may affect existing integrations. MSC Trustgate.com shall maintain deprecated API versions for a commercially reasonable transition period following such notice.

(d) Subscriber shall not attempt to circumvent, reverse-engineer, or interfere with MSC Trustgate.com's security controls, authentication mechanisms, rate limits, or access controls in connection with the cloud signing platform.

(e) Subscriber is responsible for the security of its own integration environment, including the protection of user credentials, session tokens, and document data transmitted to and from MSC Trustgate.com's API.

C6. Data Handling and Privacy

(a) Identity and credential data collected for the purposes of Subscriber authentication and certificate issuance is processed by MSC Trustgate.com as an independent data controller in accordance with MSC Trustgate.com's Privacy Policy and the Personal Data Protection Act 2010 (Act 709).

(b) Document data submitted to MSC Trustgate.com's signing infrastructure for the purpose of applying a digital signature is processed transiently and is not retained by MSC Trustgate.com beyond the duration necessary to complete the signing operation, except where retention is required by applicable law or MSC Trustgate.com's CP/CPS.

(c) Where MSC Trustgate.com processes Subscriber data in its capacity as a data processor on behalf of an enterprise or organisational Subscriber, the parties shall enter into a Data Processing Agreement (DPA) setting out the terms of such processing, consistent with the requirements of the PDPA 2010.

(d) MSC Trustgate.com shall notify Subscriber in accordance with applicable law in the event of a confirmed personal data breach affecting Subscriber's account or credential data.

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

SCHEDULE D — HARDWARE-BASED SIGNING (USB TOKENS & HSMS)

D1. Scope and Application

This Schedule applies where Subscriber generates and stores the private key corresponding to a document-signing Certificate on a cryptographic hardware device under the Subscriber's physical control, including USB cryptographic tokens and Hardware Security Modules (HSMs) operated on the Subscriber's premises or in a data centre under the Subscriber's management.

D2. Approved Device Requirements

(a) Cryptographic hardware used to store private keys under this Schedule must be certified to at minimum: - FIPS 140-2 Level 2 (for USB tokens and individual use); or - FIPS 140-2 Level 3 or FIPS 140-3 Level 3 (for organisational HSMs and high-assurance Certificate classes), or an equivalent standard under Common Criteria as specified in MSC Trustgate.com's CP/CPS.

(b) Subscriber shall not use hardware that has been modified, tampered with, or whose firmware has been altered in a manner not authorised by the device manufacturer or MSC Trustgate.com.

(c) Upon receipt of a new cryptographic token or HSM, Subscriber shall change all default PINs, passwords, and administrative credentials before first use.

(d) Subscriber shall configure the device to enforce PIN or password lockout after a maximum of five (5) consecutive incorrect authentication attempts. Where the device supports it, Subscriber should enable automatic token locking after a period of inactivity.

D3. Loss, Compromise, and Incident Response

(a) Subscriber shall immediately notify MSC Trustgate.com at compliance@msctrustgate.com upon: - Loss or theft of a cryptographic token or HSM; - Suspected compromise of a private key or the hardware containing it; - Detection of unauthorised access to, or tampering with, a cryptographic device or its operating environment; or - Any other security incident that may have affected the integrity of a private key.

(b) Upon notification of a loss or compromise, MSC Trustgate.com shall proceed with revocation of the associated Certificate in accordance with MSC Trustgate.com's CP/CPS and as described in Schedule B, Clause B8.

(c) Subscriber shall cooperate with MSC Trustgate.com in any investigation of a suspected key compromise, including providing access to relevant logs, records, and physical hardware as reasonably requested.

(d) Subscriber shall bear the cost of Certificate re-issuance necessitated by a loss or compromise attributable to Subscriber's failure to comply with the requirements of this Schedule.

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

SCHEDULE E — S/MIME (SECURE EMAIL CERTIFICATES)

E1. Scope and Application

This Schedule governs the issuance and use of Secure/Multipurpose Internet Mail Extensions (S/MIME) Certificates issued by MSC Trustgate.com for the purpose of email message signing and encryption. It applies to S/MIME Certificates for individual mailboxes, role-based accounts, and organisational gateway configurations as offered by MSC Trustgate.com from time to time.

E2. Certificate Classes and Identity Assurance

(a) Mailbox-Validated (MV) S/MIME. The applicant's control of the email address is verified. Identity of the named individual is not separately verified. Suitable for general email integrity purposes.

(b) Organisation-Validated (OV) S/MIME. In addition to mailbox control, the applicant's legal organisation is verified against official business records. Suitable for corporate communications where organisational identity is important.

(c) Individual Validated S/MIME. In addition to mailbox control validation, the Subscriber's identity is verified against a government-issued identity document or equivalent reliable data source in accordance with MSC Trustgate.com's CP/CPS. The Certificate includes the Subscriber's verified legal name and email address. Suitable for professional email communications where individual identity assurance is required, in addition to proof of email ownership.

(d) Sponsored Validated S/MIME. Issued to role-based accounts or organisational gateways on behalf of, and with the authorisation of, the employing or sponsoring organisation. The organisation warrants the accuracy of Subscriber information submitted for such Certificates.

E3. Permitted Uses

S/MIME Certificates issued under this Schedule may be used for:

(a) Digitally signing outbound email messages to provide recipients with assurance of the sender's identity and the integrity of the message content;

(b) Encrypting outbound email messages to protect message confidentiality in transit and at rest;

(c) Decrypting inbound encrypted email messages sent to the Subscriber's mailbox; and

(d) Any other purpose expressly authorised in MSC Trustgate.com's CP/CPS or in writing by MSC Trustgate.com.

E4. Revocation Triggers

Subscriber must request revocation of an S/MIME Certificate without undue delay upon the occurrence of any of the following:

(a) Compromise or suspected compromise of the private key;

(b) Loss of control of the email address associated with the Certificate;

(c) Termination of employment or change of role affecting the Subscriber's entitlement to use a role-based or sponsored S/MIME Certificate;

(d) Discovery of any material inaccuracy in the Certificate information; or

(e) Any policy violation or legal requirement necessitating revocation.

E5. Relying Party Verification

Relying Parties receiving a signed email message should, before relying on the signature:

(a) Validate the S/MIME Certificate chain up to a trusted root;

(b) Check the revocation status of the Certificate via CRL or OCSP;

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

(c) Confirm that the email address in the Certificate matches the sender address in the message header

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

SCHEDULE F — TLS/SSL (SERVER CERTIFICATES)

F1. Scope and Application

This Schedule governs the issuance and use of TLS/SSL server Certificates issued by MSC Trustgate.com for use in securing server communications. It applies to Domain Validation (DV), Organisation Validation (OV), and Extended Validation (EV) server Certificates for both public-trust and private-trust use cases, as offered by MSC Trustgate.com under its CP/CPS.

F2. Validation Types and Procedures

(a) Domain Validation (DV). MSC Trustgate.com verifies that the applicant has control over the domain(s) listed in the Certificate using one or more approved domain control validation methods, including DNS-based validation, file-based HTTP validation, or email-based validation to a domain contact address. DV Certificates provide assurance of domain control only, not organisational identity.

(b) Organisation Validation (OV). In addition to domain control, MSC Trustgate.com verifies the applicant's legal organisation against official business registry records or equivalent databases. OV Certificates include the organisation's name and provide a higher level of assurance to Relying Parties.

(c) Extended Validation (EV). MSC Trustgate.com performs enhanced identity verification in accordance with applicable EV Guidelines or MSC Trustgate.com's equivalent EV-level CP/CPS requirements. EV Certificates include additional Subject Identity Information and are suitable for applications requiring the highest level of organisational identity assurance.

F3. Certificate Profiles and Validity

(a) TLS/SSL Certificate profiles shall conform to MSC Trustgate.com's CP/CPS and, for publicly trusted Certificates, to the requirements of *Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates* applicable to publicly trusted TLS/SSL Certificates.

(b) Certificate validity periods for publicly trusted TLS/SSL Certificates shall comply with the maximum validity periods permitted under applicable *Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates* in effect at the time of issuance, which may be shorter than those stated in MSC Trustgate.com's CP/CPS if *Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates* are updated during the Certificate's life.

(c) Key sizes and algorithms shall comply with MSC Trustgate.com's CP/CPS minimum requirements. Subscriber shall not use key sizes or algorithms that fall below MSC Trustgate.com's minimum standards or that are known to be cryptographically weak at the time of use.

F4. Subscriber's Domain Control Obligations

(a) Subscriber warrants that it has the legal right to use all domain names and IP addresses listed in the Certificate and that it will maintain control over those domains throughout the Certificate's validity period.

(b) Where domain control validation requires the installation of a DNS record, HTTP validation file, or other validation artifact, Subscriber shall implement and maintain such artifacts for the duration of any automated or periodic re-validation requirement.

(c) Subscriber shall notify MSC Trustgate.com promptly if it loses control of any domain name listed in a Certificate and shall request revocation of that Certificate without undue delay.

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

F5. Server and Private Key Security

(a) Subscriber shall protect the private key associated with a TLS/SSL Certificate with security controls appropriate to the sensitivity of the data protected by the Certificate, including:

- Storage of the private key within an HSM or equivalent hardware-protected key storage where practicable;
- Access controls ensuring that the private key is accessible only to the server processes and personnel that require it;
- Immediate revocation and re-keying upon any suspected compromise of the private key.

(b) Subscriber shall configure servers using TLS/SSL Certificates issued under this Schedule to:

- Disable deprecated and cryptographically weak protocol versions (including SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1 where not required for legacy compatibility);
- Disable weak cipher suites and prioritise cipher suites providing forward secrecy;
- Enable certificate revocation checking via stapled OCSP responses where supported by the server software.

F6. Revocation

Subscriber must request revocation of a TLS/SSL Certificate without undue delay upon:

(a) Compromise or suspected compromise of the private key;

(b) Mis-issuance or discovery of inaccurate information in the Certificate;

(c) Cessation of use of the domain name listed in the Certificate; or

(d) Any other circumstance listed in MSC Trustgate.com's CP/CPS as requiring revocation.

For publicly trusted Certificates, MSC Trustgate.com may be required to revoke the Certificate within a prescribed time period following detection of certain conditions, and Subscriber shall cooperate with MSC Trustgate.com in facilitating such revocation.

F7. Liability

(a) No separate monetary warranty is provided for TLS/SSL Certificates issued under this Schedule unless a separate written warranty, Product Disclosure Statement (PDS), or Relying Party Agreement expressly provides for one.

(b) MSC Trustgate.com's liability for losses arising from a TLS/SSL Certificate is subject to the general limitations in Section 9 of the Agreement:

Certificate Class	Reliance Limit
SSL Domain Validation (non-public trusted)	RM 500
SSL Organisation Validation (non-public trusted)	RM 50,000

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.

COMMON SLA — AVAILABILITY, SUPPORT & CREDITS

Availability Target. Monthly System Availability target 95% excluding Scheduled Maintenance and Excused Downtime; measured on calendar month basis.

Support & Response. Business hours Mon–Fri, 09:00–18:00 MYT (excluding public holidays).

Maintenance. Scheduled maintenance with reasonable advance notice; emergency maintenance for security issues as needed.

© MSC Trustgate.com Sdn. Bhd. — Subscriber Agreement V.1.5, 2026. All Rights Reserved.