



Master Partner Agreement

THESE TERMS TOGETHER WITH ANY APPLICABLE PARTNER SPECIAL TERMS (THE "AGREEMENT") GOVERN YOUR USE OF THE PORTAL, AND THE MARKETING, RESALE AND/OR DISTRIBUTION OF THE PRODUCTS AND SERVICES ORDERED BY YOU UNDER ONE OR MORE ORDER SUMMARIES. YOU MUST READ THIS AGREEMENT CAREFULLY BEFORE CREATING AN ATLAS ACCOUNT. BY CHECKING THE ACCEPTANCE BOX AND CREATING AN ATLAS ACCOUNT, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU WILL NOT BE PERMITTED TO MARKET, RESELL OR DISTRIBUTE THE PRODUCTS, CREATE AN ATLAS ACCOUNT OR PLACE ANY ORDERS.

BY CHECKING THE ACCEPTANCE BOX, YOU REPRESENT AND WARRANT THAT YOU ARE DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON BEHALF OF THE COMPANY IDENTIFIED IN THE ATLAS ACCOUNT YOU ARE CREATING ("PARTNER" OR "YOU") AND TO BIND PARTNER TO THE TERMS OF THIS AGREEMENT WITH GLOBALSIGN.

1. Definitions

Administrator: A user registered in Partner's Atlas Account and who has access to perform functions on behalf of Partner and may assign other users

Affiliate: An entity that directly or indirectly controls, is controlled by, or is under common control with a party to this Agreement.

Atlas Account: The account created by Partner in Atlas for Partner's use of the Portal.

Certificate: An electronic document that uses a digital signature to bind a public key and an identity, i.e. digital certificate.

CPS: GlobalSign's Certification Practice Statement available at <https://www.globalsign.com/en/repository> as updated from time to time.

Customer: A customer of Partner who holds a Subaccount.

eIDAS Regulation: REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (European).

FlexQuota: The per unit price for a Product when Partner exceeds its Quota or continues to order Products after the end of the Product Term as shown on the Order Summary. Also may be referred to as "Overage".

GlobalSign: The GlobalSign contracting entity assigned when Partner creates its Atlas Account.

Industry Standards: The applicable (a) requirements or guidelines adopted by the CA/Browser Forum, (b) requirements applicable to GlobalSign's inclusion in a trusted root store adopted by an application software vendor, or (c) other applicable regulatory or quasi-regulatory standards, including but not limited to, the eIDAS Regulation (where applicable).

Order Summary: The order document accepted by Partner which sets out the Products and Services purchased by Partner, certain Product features, Quota and fees payable, each representing an individual purchase which is governed by this Agreement.

Partner Product Pack: A Product Pack ordered by Partner. During the Product Term, Partner may create Subaccount Product Packs, up to the value of the Quota in the Partner Product Pack, for resale to one or more of its Customers or Subresellers.

Partner Special Terms: The schedule(s) attached to this Agreement which include additional terms and conditions applicable to Partner based on the roles and permissions for the Partner Type as available to Partner in the Portal.

Partner Type: The category of partner (for example, Reseller, Service Provider, etc). that includes certain benefits and permissions made available to Partners in the Portal. Certain Partner Types may also be subject to Partner Special Terms.

Portal: The portal for the Services that provides account management and ordering tools to facilitate the management of products and services provided by GlobalSign. The Portal also includes Atlas Discovery, a Certificate lifecycle management (CLM) tool, where this feature has been enabled.

Product: The product(s) purchased by Partner shown on the Order Summary, which may include Signatures, Transactions, Certificates, timestamps and OV Certificate Identities. "Product" also includes any optional add-on features or items that may be purchased by Partner.

Product Pack: The Products ordered, up to the value of the Quota, and available for use during the Product Term. A Product Pack may be either a Partner Product Pack or an Subaccount Product Pack.

Product Term: The period in months shown on the Order Summary during which Partner may resell or distribute the purchased Products to its Customers or Subresellers.

Product Term Start Date: The date when the Product Term begins. If a Service, the Product Term Start Date is the date when the Service is activated.

Quota: The combined total quantity of Products available in a Product Pack as shown on the Order Summary.

Reseller: A Partner Type. A Reseller purchases Products to sell them rather than consume or use them itself.

Service: A hosted service, including Products, ordered by Partner as shown on an Order Summary.

Service Credentials: Any form of credential made available by GlobalSign to a Customer or Service Provider to access a Service, such as an API Credential, mTLS Certificate, or ACME MAC Key.

Service Provider: A Partner Type. A Service Provider incorporates the Products or Services into its own offerings to enhance their value proposition.

Service Schedule: The additional terms and conditions applicable to specific Products or Services ordered by a Partner according to their Partner Type

Subreseller: A reseller appointed by Partner and holds a Subaccount.

Subaccount: An Atlas Account created for a Customer or Subreseller under Partner's Atlas Account and with a limited set of the roles and permissions.

Subaccount Product Pack: A Product Pack sold by Partner to a Customer or Subreseller. A Subaccount Product Pack may have a different Product Term than the Partner Product Pack.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. If the Subject is a device or system, it must be under the control and operation of the Subscriber.

Subscriber: A natural person or legal entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement. Prior to Certificate issuance, the Subscriber is referred to as the "Applicant". For Certificates issued to devices, the Subscriber/Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate request.

Subscriber Agreement: An agreement between the CA and the Subscriber that specifies the rights and responsibilities of the

parties available at https://www.globalsign.com/en/repository/GlobalSign_Subscriber_Agreement.pdf as updated from time to time.

Territory: The territory shown in the table below where Partner is permitted to market and resell/distribute the Products.

Test Product: An untrusted or non-production version of a Product made available for Partner's use solely for evaluation or trial purposes, including proofs of concept, beta or other testing, and/or at no charge to Partner.

TPS: The GlobalSign Timestamping Practice Statement available at https://www.globalsign.com/en/repository/GlobalSign_TPS_v1.0_final.pdf as updated from time to time.

Trial Product: A production ready version of a Product made available for Partner's use for evaluation purposes and/or at no charge to Partner.

Any capitalized terms used in this Agreement or the Service Schedule(s) but not otherwise defined herein shall have the meaning set forth in the CPS, Subscriber Agreement, or TPS (if applicable).

2. License; Use of the Portal.

GlobalSign appoints Partner as a non-exclusive partner to (i) market and distribute Products in the Territory to Customers, and (ii) appoint Subresellers, in accordance with the terms of this Agreement and any applicable Partner Special Terms. Partner shall not market and distribute the Products to Customers located in countries outside the Territory without the prior written consent of GlobalSign. Partner's marketing and/or distribution of the Products outside of the Territory without prior written consent shall be a material breach of this Agreement.

GlobalSign Contracting Entity	Territory
GMO GlobalSign K.K.	Japan
GMO GlobalSign Ltd	UK, EU, Africa
GMO GlobalSign NV	UK, EU, Africa
GMO GlobalSign, Inc. (US)	North America and South America
GMO GlobalSign Pte Ltd	Asia Pacific, South Korea, Taiwan
GMO GlobalSign Inc. (Philippines)	Philippines
GMO GlobalSign Certificate Services Pvt Ltd	India, Middle East
GMO GlobalSign China Co., Ltd.	China
GMO GlobalSign Russia LLC	Russia and CIS Countries
GMO GlobalSign Solutions in Technology S/A	Brazil
GMO GlobalSign FZ LLC	Gulf countries

If Partner uses the Products or Service for its own internal use, such use is subject to the terms of the GlobalSign Master Services Agreement ("MSA") available at <https://www.globalsign.com/en/repository/Master-Services-Agreement.pdf>. For clarity, Partner's use of the Service in its capacity as a Service Provider is further subject to the Partner Special Terms and applicable Service Schedule and not the MSA.

2.1 Use of the Portal. In connection with the Services, Partner will have access to the Portal after Partner's creation of an Atlas Account. In the Portal, the Administrator may perform functions such as purchasing Products, accepting sales quotes, requesting identities, and obtaining Service Credentials (if applicable). The Portal may also provide certain communications from GlobalSign, such as service announcements and other messages. Partner is responsible for maintaining the confidentiality of any Service Credentials held by Partner and is fully responsible for all activities that occur under Partner's Atlas Account. Partner must (a) immediately notify GlobalSign of any unauthorized use of its Service Credentials or any other breach of security to support@globalsign.com, and (b) ensure that Partner logs out from its Atlas Account at the end

of each session. GlobalSign may deactivate or remove Partner's Atlas Account and/or access to the Portal if Partner has not conducted any transactions for one (1) year or more.

3. Limitations on Use. Partner shall not: (a) copy, modify or create derivative works of the Products or Services or any component thereof; (b) host, time-share, rent, lease, sell, resell, transfer, license, sublicense, assign, distribute or otherwise make available the Services (including any Products) to any third party, except as permitted under this Agreement and the Partner Special Terms; (c) disassemble, decompile, reverse engineer or otherwise attempt to discover the source code of the Products or Services; (d) use the Services to send or store infringing or unlawful material or viruses, worms, time bombs, Trojan horses and other harmful or malicious codes, files, scripts, agents or programs; or (e) use the Services except as permitted under this Agreement and in compliance with all applicable Industry Standards, laws and regulations.

4. Customer and Subreseller Agreements. The Products and Services are provided to Customers and Subresellers in accordance with GlobalSign's applicable terms of use. Partner shall ensure that each Customer and/or Subreseller has access to and accepts the terms of use, either (i) as provided by GlobalSign via the Portal or (ii) by Partner entering into its own agreement with the Customer and/or Subreseller that contains terms and conditions that are substantially similar to the terms for Subaccounts available at <https://www.globalsign.com/en/repository> (the "Terms for End Users of Subaccounts") as may be updated by GlobalSign from time to time. If the Customer and/or Subreseller requests Publicly Trusted Certificates, the End Terms for Subaccount Users also include the Subscriber Agreement and CPS. Partner shall enforce the terms of use against its Customers and Subresellers. GlobalSign may, from time to time, in its reasonable discretion, request that Partner provide to GlobalSign copies of its executed Customer Agreements to ensure compliance with this Section 4. If Partner has appointed a Subreseller, Partner shall enter into an agreement with the Subreseller that (i) includes terms and conditions no less protective of GlobalSign than the terms of this Agreement, and (ii) requires the Subreseller to flow down the terms of this Section 4 to its end customers.

5. Test Trial Products. The terms of this Section 5 apply if Partner is granted the right to use a Test Trial Product.

5.1 Trial Product. Partner may use Trial Products solely for the purpose of its evaluation of a Product. Partner's right to use Trial Products will terminate immediately upon the earlier of (a) the date the number of Trial Products in the Product Pack is depleted, or (b) the date when GlobalSign terminates Partner's right to use the Trial Products (which GlobalSign may do at any time in its sole discretion).

5.2 Test Service. Partner may only use a Test Product for test purposes in a non-production, test environment, and solely for the purpose of Partner's internal evaluation and interoperability testing of a Service. Partner's right to use a Test Product will terminate immediately upon the earlier of (a) the date the number of Products in the Product Pack is depleted, (b) the expiration date of the Product Term, or (c) the date when GlobalSign terminates Partner's right to use a Test Product (which GlobalSign may do at any time in its sole discretion).

5.3 Warranty Disclaimer for Test or Trial Products. PARTNER ACKNOWLEDGES THAT ANY TEST OR TRIAL PRODUCTS ARE PROVIDED SOLELY FOR EVALUATION OR TEST PURPOSES. EXCEPT AS PROVIDED IN THE CPS OR TPS AT <https://www.globalsign.com/en/repository>, TEST AND TRIAL PRODUCTS ARE PROVIDED "AS IS" AND WITHOUT ANY WARRANTY WHATSOEVER. TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW, GLOBALSIGN EXPRESSLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT, RELATING TO THE TEST OR TRIAL PRODUCTS, PARTNER'S USE OR ANY INABILITY TO USE THE TEST OR TRIAL PRODUCTS, THE RESULTS OF THEIR USE AND THIS AGREEMENT.

5.4 LIMITATION OF LIABILITY FOR TEST AND TRIAL PRODUCTS. GLOBALSIGN SHALL NOT BE LIABLE TO PARTNER OR ANY THIRD PARTY FOR ANY CLAIMS, DEMANDS OR DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DIRECT, INDIRECT, CONSEQUENTIAL OR SPECIAL DAMAGES, ARISING OUT OF THE USE OF THE TEST OR TRIAL PRODUCTS AND THE USE OR FAILURE OF THE TEST OR TRIAL PRODUCTS TO OPERATE FOR WHATEVER REASON, WHETHER IN SUCH ACTION IS BASED IN CONTRACT OR TORT OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, NEGLIGENCE.

6. Product Packs; Fees; Payment.

6.1 Product Packs; FlexQuota. Partner may distribute Subaccount Product Packs to its Customers and Subresellers. All Product Packs expire at the end of the applicable Product Term. There is no credit or refund for unused Products in a Product Pack. If Partner wishes to continue to resell Products after the end of the Product Term, or if Partner exceeds its Quota, Partner may order a new Product Pack or order Products individually at the FlexQuota price. GlobalSign reserves the right to adjust FlexQuota prices at any time following one (1) year after the end of the Product Term.

6.2 Fees; Payment. Partner agrees to pay GlobalSign the fees for the Products and/or Services shown in any Order Summary. Partner shall pay in full all amounts due in the Order Summary regardless of whether Partner receives payment from the applicable Customer or Subreseller.

6.2.1 Partner shall provide GlobalSign with valid, up-to-date and complete credit card details or, if applicable, purchase order information acceptable to GlobalSign. If Partner provides its credit card details to GlobalSign, Partner hereby authorizes GlobalSign to charge such credit card for the fees due. If Partner provides purchase order information to GlobalSign, and/or opts to pay by invoice, GlobalSign shall invoice Partner for the fees due.

GlobalSign will invoice/charge Partner (i) on the Effective Date for the Grand Total in the Order Summary for the initial order, and (ii) on the Order Date for the Grand Total in the Order Summary for subsequent orders. GlobalSign will invoice Partner or charge Partner's credit card (as applicable) for any recurring fees in accordance with the billing frequency shown on the Order Summary.

If Partner orders Products individually (whether after the end of the Product Term or on a pay-as-you-go basis), GlobalSign will invoice/charge Partner on a monthly basis in arrears at the FlexQuota price shown for the Product on the Order Summary.

6.2.2 All payments are payable in the currency on the Order Summary and, unless otherwise set forth on the Order Summary, are due net thirty (30) days from the invoice date. GlobalSign's quoted prices for the Services and Products are exclusive of any and all taxes or duties. Such taxes and duties, when applicable, will be added to the invoices. Partner will pay any taxes, fees and similar governmental charges related to the execution or performance of this Agreement, other than applicable income taxes imposed on GlobalSign related to its receipt of payments from Partner.

6.2.3 If any undisputed invoiced amount is not received by GlobalSign by the due date, then without limiting GlobalSign's rights or remedies, those charges will accrue late interest at the rate of 1.5% of the outstanding balance per month, or the maximum rate permitted by law, whichever is lower. GlobalSign may suspend or limit Partner's access to the Portal or Service without notice until full payment is made and revoke any previously issued Certificates. Partner must notify GlobalSign of any fee disputes within thirty (30) days of the applicable invoice date or such invoice will be deemed accepted.

7. Term; Termination. The term of this Agreement will begin on the date accepted by Partner (the "Effective Date") and will continue for a period of one (1) year unless terminated earlier as provided herein. This Agreement shall automatically renew on the same terms and conditions for successive one (1) year periods unless either party gives the other written notice of termination at least sixty (60) days prior to the end of the then current term.

7.1 Termination.

7.1.1 *By either party:* Either party may terminate this Agreement immediately upon written notice if the other party (a) is in breach of Section 10 (Confidentiality); (b) files for bankruptcy, ceases to carry on business, or undergoes liquidation; (c) is unable to perform a material portion of its obligations under this Agreement or any Service Schedule as a result of an event or events of force majeure for a period of not less than thirty (30) days;

7.1.2 *By GlobalSign:* This Agreement may be terminated by GlobalSign upon written notice to Partner (a) if Partner materially breaches this Agreement and such breach continues for a period of thirty (30) days after notice thereof has been

given by GlobalSign; or (b) at any time upon no less than ninety (90) days' written notice to Partner. Notwithstanding the foregoing, this Agreement may be terminated immediately by GlobalSign upon written notice if GlobalSign determines, in its reasonable discretion, that Partner has breached Sections 2, 9.1 or 11.1 or poses a security or compliance risk to the Services or GlobalSign.

8. Effect of Termination. Upon termination or expiration of this Agreement, all rights, licenses and obligations of the parties under this Agreement shall cease immediately. Notwithstanding the foregoing, Customers of a Reseller may continue to use Product Packs purchased prior to termination, provided Reseller is not in breach of this Agreement and the applicable Customer is not in breach of its Customer Agreement. The following Sections shall survive any expiration or termination of this Agreement: 1, 6.2, 7, 8, 10 – 16 and 19 of this Agreement and "Audit Rights" in any applicable Service Schedule.

9. Warranty and Disclaimer

9.1 Compliance with Laws. Each party warrants that it shall comply with all federal, state, and local laws and regulations applicable to GlobalSign's provision and/or use of a Service or Product. Each party shall comply, at its own expense, with all sanction laws, import and export laws, restrictions, national security controls, and regulations of any applicable country's agency or authority (collectively "Laws"). Each party warrants that it is not designated or otherwise subject to economic sanctions or other restrictions pursuant to the Laws and that no individual or entity designated or otherwise subject to economic sanctions under the Laws owns a 50% or more interest in such party, and does not control such party, directly or indirectly. Such warranty is continuing in nature and each party shall advise the other party immediately of any change that affects this warranty. Neither party shall import, export, re-export, or authorize the export or re-export of the Services or any other product, technology or information that it obtains or learns of hereunder, or any copy or direct product thereof, in violation of any Laws, or without any required license or approval.

9.2 Authority. Each party warrants that it is validly existing and in good standing under the laws of the jurisdiction of its organization and has the power and authority to enter into this Agreement and that this Agreement has been duly executed and delivered by such party and constitutes the valid and binding obligation of such party.

9.3 Personal Data. Partner may provide GlobalSign with information needed for the provision of Products or Services to Customers. This information may include personal data. Partner will inform Customers about the information Partner will provide to GlobalSign, how the information will be used, and obtain any consents required for the collection, transfer and use of such information by GlobalSign as stated in the GlobalSign privacy policy at <https://www.globalsign.com/repository/>. Partner warrants that (i) it has the necessary rights to provide any personal data or other information that Partner provides to GlobalSign, and (ii) providing such information does not violate any applicable data privacy law, contract or privacy policy. The terms of the GlobalSign data processing addendum at <https://www.globalsign.com/en/repository/GlobalSign-DPA-For-Partners.pdf> ("DPA") are hereby incorporated by reference and shall apply to the extent GlobalSign processes any Partner and Customer Personal Data, as defined in the DPA.

9.4 No Other Warranty. EXCEPT AS OTHERWISE PROVIDED IN THE SUBSCRIBER AGREEMENT OR CPS, TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW, GLOBALSIGN, ITS AFFILIATES, AND THEIR RESPECTIVE SUCCESSORS, DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS DISCLAIM ALL OTHER WARRANTIES AS TO THE USE, DELIVERY, LICENSE, PERFORMANCE OR NONPERFORMANCE OF, USE OR INABILITY TO USE THE SERVICES, PRODUCTS, THIRD PARTY PRODUCTS, CERTIFICATES, SOFTWARE, DOCUMENTATION OR ANY OTHER SERVICES OFFERED OR CONTEMPLATED BY THIS AGREEMENT, EXPRESS OR IMPLIED. GLOBALSIGN, ITS AFFILIATES, AND THEIR RESPECTIVE SUCCESSORS, DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS EXPRESSLY DISCLAIM ALL REPRESENTATIONS AND WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. GLOBALSIGN DOES NOT WARRANT THAT THE SERVICE OR ANY PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE.

10. Confidentiality. "Confidential Information" means all information that is provided or made available to one party (the "Receiving Party") by the other party (the "Disclosing Party"). Confidential Information includes, but is not limited to:

inventions, technologies; strategies; trade secrets; customer and supplier lists; product designs and pricing information; processes; formulas; business plans; employer and consumer information; employee data; product licensing plans; budgets, finances, and financial plans; production plans and protocols; technology infrastructure; information security systems, policies and practices, and technology, data, and methods, and any other information that by its nature would typically be considered non-public information. Confidential Information may be conveyed to the Receiving Party in written, electronic, or oral form, and includes any information that may be derived from or developed as a result of access to the Disclosing Party's facilities, as well as all notes, reports, evaluative materials, analyses or studies prepared by the Receiving Party or its directors, officers, employees, agents and advisors (collectively, such Party's "Representatives") regarding or relating to the Disclosing Party or its Confidential Information.

The Receiving Party will protect, and will ensure its employees, officers, agents and contractors will protect Confidential Information by using the same degree of care as Receiving Party uses to protect its own Confidential Information of a like nature (but no less than a reasonable degree of care) to prevent the unauthorized use, dissemination, disclosure or publication of such Confidential Information. The Receiving Party may disclose the Confidential Information only to those of its Affiliates and their respective employees and advisors who have a need to know and who are under an obligation of confidentiality at least as restrictive as that contained herein. GlobalSign may also disclose Confidential Information as may be required for GlobalSign to fulfill its obligations under applicable Industry Standards, subject to appropriate confidentiality provisions. Confidential Information received may be used only to fulfill the purposes of the Agreement. If a Receiving Party or any of its respective Affiliates is requested or required by subpoena, court order, or similar process or applicable governmental regulation to disclose any Confidential Information, Receiving Party agrees to provide the Disclosing Party with prompt notice of such request or obligation so that the Disclosing Party may seek an appropriate protective order or procedure if it elects to do so.

The foregoing confidentiality obligations will not apply to Confidential Information that (a) is now or subsequently becomes generally available to the public through no fault or breach on the part of the Receiving Party; (b) is known by the Receiving Party prior to disclosure as noted by tangible record; (c) is independently developed by the Receiving Party without the use of any Confidential Information of the Disclosing party; (d) the Receiving Party rightfully obtains without a duty of confidentiality from a third party who has the right to transfer or disclose it; (e) is disclosed under operation of law; or (f) is disclosed by the Receiving Party with the prior written approval of the disclosing party.

Upon termination of this Agreement, the Receiving Party shall return or destroy the Disclosing Party's Confidential Information upon the Disclosing Party's request. The Receiving Party shall be permitted to retain copies of the Disclosing Party's Confidential Information to the extent necessary to comply with legal, compliance and/or document retention requirements. Any Confidential Information so retained will remain subject to the obligations and restrictions contained in this Section, notwithstanding any termination hereof, and the Receiving Party will not use the retained Confidential Information for any other purpose.

11. Ownership; Use of Logos, Trademarks, and URLs. Except for the rights expressly granted under this Partner Agreement, all right, title and interest in and to the Service, Products, APIs, and Portal are owned exclusively by GlobalSign. GlobalSign retains all right, title, and interest in and to the Service and all other products, software, documentation, works, and other intellectual property created, used, or provided by GlobalSign for the purposes of this Agreement, and all modifications, improvements and derivative works of the same.

11.1 Each party grants the other party a limited license during the term of this Agreement to use the party's corporate logo, name, trademark, URL, and product names (the "Names") on the its web site for listing the party as a provider/distributor of the Products and to promote the Products. In using the GlobalSign names, Partner shall comply with GlobalSign's "Branding Guidelines for Partners" at <https://www.globalsign.com/en/company/corporate-policies/>. Either party may withdraw this limited license at any time upon reasonable notice to the other party. Other than the rights granted in this Section, neither party has any other rights to the Names of the other party. Partner will not: (i) use, register or attempt to register any GlobalSign Names as its own, (ii) use, register, or attempt to register any name, logo, mark, domain name or other identifier which is likely to lead to confusion with the GlobalSign Names, (iii) use the GlobalSign Names in a manner likely to disparage or misrepresent GlobalSign, or (iv) use the GlobalSign Names in a manner not expressly permitted by this Agreement.

11.2 In order to support its Customers, Partner may, at its own expense, translate GlobalSign's marketing materials and support documentation into other languages in the Territory. GlobalSign shall own all rights and title to all such translations, and Partner hereby assigns any and all rights it may have to any translations to GlobalSign. Partner shall include GlobalSign's copyright notice on all translations and copies at no cost to GlobalSign. Partner shall provide GlobalSign with copies of translated documents upon GlobalSign's request and shall, at its own expense, make any corrections reasonably requested by GlobalSign.

12. Indemnification

12.1 Partner will settle and/or defend at its own expense and indemnify and hold harmless GlobalSign against any cost, loss or damage from any claim, demand, suit or action brought by a third party against GlobalSign arising out of or related to any (i) any claim by a Customer alleging that Partner accessed or used the Customer's account without authorization from the Customer, outside of the scope of its express authority or in contravention of instructions given by the Customer, (ii) breach of this Agreement by Partner, or (iii) if Partner is a Service Provider, the purchase or use of the Service or Products by a third party who is accessing or acquiring the Service or Product through Partner, including any Customers or Subresellers.

12.2 The party seeking indemnification (the "Indemnified Party") agrees to promptly notify the party providing indemnification (the "Indemnifying Party") in writing of any indemnifiable claim. The Indemnifying Party shall control the defense and settlement of an indemnifiable claim. The Indemnified Party shall cooperate in all reasonable respects with Indemnifying Party and its attorneys in the investigation, trial, defense and settlement of such claim and any appeal arising therefrom. The Indemnified Party may participate in such investigation, trial, defense and settlement of such claim and any appeal arising therefrom, through its attorneys or otherwise, at its own cost and expense.

13. Limitation of Liability. GlobalSign, its Affiliates, and their respective successors, directors, officers, employees, and agents' aggregate liability to Partner for any and all claims arising out of or relating to this Agreement, or the use of or inability to use the Services or Products, will in no event exceed the amount of fees paid by Partner for Product Packs within the one (1) year period immediately prior to the event that gave rise to its claim.

14. Limitation of Damages. In no event shall GlobalSign, its Affiliates, and their respective successors, directors, officers, employees, and agents be liable to Partner or any third party for any special, consequential, incidental or indirect damages including, but not limited to, loss of profits, revenue, or damage to or loss of data arising out of or relating to this Agreement or the use of or inability to use the Services or Products whether or not GlobalSign has been advised of the possibility of such damages.

15. Governing Law and Jurisdiction. The (i) laws that govern the interpretation, construction, and enforcement of this Agreement and all matters, claims or disputes related to it, including tort claims, and (ii) the courts that have exclusive jurisdiction over any of the matters, claims or disputes, are set forth in the table below.

GlobalSign Entity on Order Summary	Governing Law	Venue
GMO GlobalSign K.K.	Japan	Tokyo District Court, Japan
GMO GlobalSign China Co., Ltd.	China	Shanghai, China
GMO GlobalSign Ltd.	England and Wales	London, England
GlobalSign NV	Belgium	Leuven, Belgium
GMO GlobalSign, Inc. (US)	New Hampshire, USA	State and federal courts of New
GMO GlobalSign Pte. Ltd	Singapore	Singapore
GMO GlobalSign Inc.	Philippines	Makati City, Philippines
GMO GlobalSign Certificate Services Pvt. Ltd	Laws of Republic of India	Delhi, India
GMO GlobalSign Russia LLC	Russia Federation Laws	Moscow, Russia
GMO GlobalSign Solutions in Technology S/A	Brazil	Belo Horizonte, Brazil

GMO GlobalSign FZ LLC	United Arab Emirates	Dubai, United Arab Emirates
-----------------------	----------------------	-----------------------------

16. Miscellaneous

16.1 Force Majeure. Neither party shall be liable for failure or delay in performing its obligations hereunder if such failure or delay is due to circumstances beyond its reasonable control, including, without limitation, acts or measures of any governmental body, war, insurrection, sabotage, embargo, pandemic, fire, flood, strike or other, interruption of or delay in transportation, unavailability of interruption or delay in telecommunications or third party services ("Force Majeure"); provided however, that if a party suffering a Force Majeure event is unable to cure that event within thirty (30) days, the other party may terminate this Agreement.

16.2 Notices. Notices shall, unless otherwise specified herein, be in writing and may be delivered by (i) hand delivery, regular mail, or overnight courier service to GlobalSign's address and Partner's "Sold To" address on the Order Summary, or (ii) email to GlobalSign to legal@globalsign.com and to Partner to the email for Partner's Primary Contact identified in Partner's Account. Notices shall be effective at the close of business on the day actually received, if received during business hours on a business day, and otherwise shall be effective at the close of business on the next business day. A party may change its contact information by providing notice of same in accordance herewith.

16.3 Assignment. Except as otherwise provided herein, this Agreement shall be binding upon, and inure to the benefit of, the successors, executors, heirs, representatives, administrators and assigns of the parties hereto. This Agreement may not be transferred or assigned by Partner without GlobalSign's prior written consent. Any such purported transfer or assignment shall be void and of no effect and shall permit GlobalSign to terminate this Agreement.

16.4 Severability. If and to the extent that any court holds any provision of this Agreement to be unenforceable, such unenforceable provision shall be stricken and the remainder of this Agreement shall not be affected thereby. The parties shall in good faith attempt to replace any unenforceable provision of this Agreement with a provision that is enforceable and that comes as close as possible to expressing the intention of the original provision.

16.5 Waiver. No waiver under this Agreement shall be valid or binding unless set forth in writing and duly executed by the party against whom enforcement of such waiver is sought. Any such waiver shall constitute a waiver only with respect to the specific matter described therein and shall in no way impair the rights of the party granting such waiver in any other respect or at any other time.

16.6. Relationship of Parties. The Parties to this Agreement are independent contractors and nothing in this Agreement shall be deemed or constructed as creating a joint venture, partnership, agency relationship, franchise, or business opportunity between GlobalSign and Partner. Neither party, by virtue of this Agreement, will have any right, power, or authority to act or create an obligation, express or implied, on behalf of the other party.

17. Entire Agreement. This Agreement, Partner Special Terms and any documents incorporated herein by reference constitute the entire agreement between the parties and supersede any prior written or oral agreement or understanding with respect to the subject matter thereof, including without limitation, the Atlas Discovery Terms of Use. The terms of this Agreement (including the Order Summary), the Subscriber Agreement, CPS and TPS (if applicable) prevail over any terms or conditions contained in any other documentation and expressly exclude any of Partner's general terms and conditions contained in any purchase order or other document issued by Partner. In the event of any conflict between the terms of the Order Summary, this Agreement, the Subscriber Agreement, CPS, TPS, and the terms of any purchase order or any other document issued by Partner, the order of precedence shall be: the Order Summary, this Agreement, the Subscriber Agreement, CPS and TPS (if applicable).

18. Amendment. GlobalSign may amend: the CPS, TPS or the Subscriber Agreement and will give notice of any material changes by posting a new version on the Portal, the GlobalSign website or by a means set forth in Section 16.2 (Notices).

19. Language. This Agreement is drafted in the English language. Any notice given under or in connection with this

Agreement shall be in English. All other documents provided under or in connection with this Agreement shall be in English or accompanied by a certified English translation. The English language version of this Agreement and any notice or other document relating to this Agreement shall prevail if there is a conflict.

20. Third Party Beneficiaries. This Agreement benefits solely the parties to this Agreement and their respective permitted successors and assigns and nothing in this Agreement, express or implied, confers on any other person any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Agreement.

Partner Agreement v 1.0 July 23, 2025

Partner Special Terms for Service Providers

If Partner is a Service Provider, these Partner Special Terms for Service Providers apply. In addition, the Service Schedule(s) for the applicable Service used by Service Provider in support of its SP Customers also apply.

1. Definitions

ACME MAC Key: An authentication code used for ACME external account binding between Service Provider's ACME Account and Service Provider's Atlas Account.

API Credentials: An authentication method comprised of a key and secret used by Service Provider or SP Customer to access a Service.

Application or App: An application designed for a mobile device (such as a smartphone). App also includes any integration or connector that may be made available by GlobalSign to assist Service Provider in accessing or integrating the Service with a Third Party Product. Apps may be subject to separate terms and conditions.

Identity Document: A physical or electronic form of identification issued by a local country or state government or passport, national ID card or other official identity document with the same level of confidence in the identity.

Individual: A natural person.

mTLS Certificate: A Certificate used for mutual or two-way authentication to a Service if Service Provider is integrating its application directly to a Service API.

Organization Validated (OV) Certificate Identity: A pre-approved Certificate identity that restricts Certificate request and issuance to a specific organization for which GlobalSign has authenticated the organization identity as described in the CPS.

Service API: An application programming interface (API) that facilitates the integration of a Service with Service Provider's internal systems, as may be made available by GlobalSign under this Agreement.

Signer: An Individual who applies a Signature acting as the Subject if the Subject is a natural person or on behalf of the Subject if the Subject is a legal person.

SP Customer: A Customer of Service Provider that either uses the Service via an interface made available by Service Provider or outsources its Certificate lifecycle

management functions to Service Provider.

Third Party Product: Any separately downloadable or accessible plug-in or Application that adds features or functionality to the Service, supports interoperability or integration and is made available by a third party as part of, in connection with, or for use with the Service.

2. License. In addition to the rights granted in Section 2 (License; Use of the Portal) above and subject to the applicable Service Schedule(s), GlobalSign grants to Service Provider the right to make the Service available to a SP Customer via an interface made available to the SP Customer by Service Provider or act as an outsource provider of Certificate lifecycle management functions for a SP Customer.

GlobalSign further grants to Service Provider a non-exclusive, non-transferable, non-sublicensable, revocable license during the term of this Agreement to use and make calls to/from a Service API solely for the purpose of facilitating Service Provider's use of a Service for the benefit of SP Customers and Service Provider's own use.

In addition to any specific use limitations that may be set forth in these Partner Special Terms, GlobalSign may set and enforce limits for reasonable use in order to prevent abuse of or undue burden on the Services.

3. Third Party Products. In connection with a Service, GlobalSign may make available or provide access to Third Party Products as a convenience for Service Provider. Service Provider's use of a Third Party Product may be subject to separate terms and conditions applicable to that Third Party Product (such as license terms of the providers of such Third Party Product). If Service Provider installs or enables or directs or otherwise authorizes GlobalSign to install or enable any Third Party Products for use with the Services where the interoperation includes access by the third party to Service Provider Confidential Information, including but not limited to, any Service Credentials, Service Provider hereby authorizes GlobalSign to allow the third party to access SP Customer Confidential Information as necessary for interoperation. Service Provider agrees that GlobalSign shall have no responsibility or liability to Service Provider for (i) any disclosure to or use by the third party of such

Confidential Information, or (ii) the use, interoperability or availability of any Third Party Products.

3. Account Setup. Where applicable, Service Provider must provide GlobalSign with point of contact information for each SP Customer for GlobalSign to provide account setup documents for the SP Customer's completion before GlobalSign will perform the authentication steps required to create an Organization Validated (OV) Certificate Identity for the SP Customer under Service Provider's account.

4. Subscriber Information. Service Provider warrants that all information and representations made by the Subscriber are true.

5. Indemnification. Subject to Section 12.2 above, GlobalSign will settle and/or defend at its own expense and indemnify and hold harmless Service Provider against any cost, loss or damage from any claim, demand, suit or action brought by a third party against Service Provider alleging that Service Provider's use of the Services as permitted hereunder infringes upon any copyright, trademark, trade secret, United States or European patent or other intellectual property right of any third party.

Should the Services become, or in GlobalSign's sole opinion likely to become, the subject of any claim or action for infringement, GlobalSign may (a) procure, at no cost to Service Provider, the right for Service Provider to continue using the Services as contemplated hereunder; (b) modify the Services, without loss of material functionality or performance, to render the Services non-infringing; or (c) if the foregoing alternatives are not reasonably available to GlobalSign, terminate this Agreement. GlobalSign's indemnification obligation will not apply to infringement actions or claims to the extent that those actions or claims are based on or result from: (i) modifications made to the Services by or on behalf of Service Provider, or (ii) the combination of the Services with items not supplied by GlobalSign, including any Third Party Products.

In addition to Section 8 above, upon termination or expiration of this Agreement, (1) Service Provider and its SP Customers shall discontinue use of the applicable Services, and (2) GlobalSign will cease providing validation services for any Service Provider Private Root CAs and ICAs, i.e. OCSP or CRL and immediately revoke all Certificates and issuing CAs unless Service Provider requests continuation of validation services and pays the applicable annual hosting fees.

Service Schedule to Partner Special Terms for Service Providers for Digital Signing Service (DSS), Qualified Trust Seals from DSS and Timestamps

This Service Schedule applies only if Partner is a Service Provider AND is purchasing DSS, Qualified Trust Seals from DSS or timestamps (as shown on an Order Summary) or Digital Signature Transactions using GMO Sign.

1. Definitions

AATL Technical Requirements: The version of the Adobe Approved Trust List Technical Requirements available at https://helpx.adobe.com/content/dam/help/en/acrobat/kb/approved-trust-list2/jcr_content/main-pars/download-section/download-1/aatl_technical_requirements_v2.0.pdf as may be updated from time to time.

AATL Timestamp: An RFC3161 compliant timestamp from GlobalSign issued by the AATL CA.

Adobe Approved Trust List (AATL): A document signing certificate authority trust store created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 9.0 and later.

Advanced Electronic Seal: An electronic seal which meets the requirements set out in Article 36 of the eIDAS Regulation.

Digital Signature: Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity and is applied by Individuals. A Digital Signature is a type of Electronic Signature that uses a Certificate to sign the document. DSS supports two types: Individual External Identities (via offline purchase) and Individual Internal Identities.

Electronic Seal: Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity and is applied in the name of a legal entity (business or organization).

Electronic Signature: An electronic sound, symbol, or process attached to or logically associated with a document and adopted by an Individual with the intent to sign a document.

ID Source: Any of (i) an Identity Document; (ii) copy of an attestation from an appropriate notary or Trusted Third Party that s/he has verified the Individual identity based on an Identity Document; or (iii) copy of a video

recording of the verification of Individual identity using secure video communication.

Identity Verification Process: The method used by a SP Customer to verify the identity of an Individual, including the setup, ID Sources, security procedures, and other implementation details. The Identity Verification Process must comply with the AATL Technical Requirements.

Individual Internal Identities: The identity of an Individual who is an employee or contractor affiliated with SP Customer's Organization Validated (OV) Certificate Identity.

Qualified Certificate for Electronic Seal: A Certificate for an electronic seal that meets the requirements laid down in Annex III of the eIDAS Regulation.

Qualified Timestamp: An RFC3161 compliant timestamp which meets the requirements of the eIDAS Regulation.

Qualified Trust Seal (QTSeal): An Advanced Electronic Seal based on a Qualified Certificate for Electronic Seal.

SEIKO Timestamp: An RFC3161 compliant timestamp accredited by the Government of Japan and provided by SEIKO.

Signature: An Electronic Signature or Electronic Seal.

Trusted Third Party: A third party approved by GlobalSign that maintains a secure process used by SP Customer for its Identity Verification Process as may be permitted by the AATL Technical Requirements.

2. Products

2.1 Digital Signing Service. In order to use DSS, Service Provider must (i) submit each SP Customer's organization identity information for verification by GlobalSign to create the SP Customer's OV Certificate Identity, (ii) purchase a Product Pack, and (iii) enroll for a mTLS Certificate if Service Provider is integrating its application directly to the DSS API. Separately, SP Customer must agree to the onboarding document as provided by GlobalSign. There are three Signature configuration

options available for DSS: (a) Signatures for Individual Internal Identities; (b) Signatures for Individual External Identities (via offline purchase); and (c) Electronic Seals.

Use of Certificates for digital signing must comply with Industry Standards and the AATL Technical Requirements. GlobalSign reserves the right to require changes to, or revoke its approval of, SP Customer's Identity Verification Process in order to comply with the AATL Technical Requirements. Service Provider shall require that SP Customer promptly implements any requested changes or immediately ceases use of DSS if requested by GlobalSign.

2.2 Qualified Trust Seals from DSS. In order to use QTSeals from DSS, You must (i) submit each SP Customer's organization identity information for verification by GlobalSign to create the OV Certificate Identity, (ii) purchase a QTSeals Product Pack, and (iii) enroll for a mTLS Certificate if Service Provider is integrating its application directly to the DSS API.

2.3 Timestamps. GlobalSign offers three types of timestamps: AATL, SEIKO, and Qualified. A DSS or QTSeals Product Pack includes timestamps equal in number to two times the Quantity of Signatures or QTSeals (as applicable) purchased in the Product Pack. Additional timestamps may be purchased with a DSS Product Pack, a QTSeals Product Pack or as a standalone Product Pack.

2.4 Qualified Timestamps. If a Product Pack includes Qualified Timestamps, GlobalSign will operate in accordance with the TPS, the CP/CPS, and any other relevant operational policies and procedures including the relevant stipulations of the eIDAS Regulation.

3. Limitations on Use. Unless Service Provider has purchased a higher rate limit, Service Provider shall not request (i) more than five (5) Signatures per second, or (ii) the creation of more than five (5) Individual Identities or Electronic Seals every five (5), or (iii) the creation of more than one QTSeal every five (5) seconds. If Service Provider exceeds the rate limit, GlobalSign may limit access to the defined rate and in the case of excessive usage or abuse, terminate this Service Schedule for breach.

Service Provider may not request more than the number of timestamps purchased in a Product Pack. Service Provider shall not request more than five (5) AATL or Qualified timestamps per second or one (1) SEIKO timestamp per second. Service Provider or its SP Customer shall be responsible for applying any

timestamps into the documents or code using the URL provided by GlobalSign. Service Provider shall maintain the confidentiality of the URL and not share it with any third parties other than SP Customers.

4. Service Provider DSS and QTSeals from DSS Obligations

4.1 If a SP Customer is using a Certificate hierarchy chained to a GlobalSign Public Root, the Certificates and Service shall be provided in accordance with the CPS.

4.2 The following obligations apply to DSS and QTSeals from DSS with the exception of 4.2 (d), (e) and (g) which do not apply to QTSeals from DSS.

Service Provider shall: (a) ensure all key activations and key pairs are controlled by the Signer and access to private keys are based on a two-factor authentication (2FA) process; (b) ensure that information provided on the enrollment requests is complete and accurate; (c) be solely responsible for developing or integrating the digitally signed hash and timestamp into Service Provider's document management system by either using the DSS API or software developer kit (SDK) or configuring DSS for Service Provider's own document workflow integration; (d) provide written evidence of compliance with the AATL Technical Requirements as may be requested by GlobalSign from time to time; (e) confirm with the Subscriber that the information is correct before approving a Certificate request; and (f) request revocation of a Certificate when any information related to the Certificate request has changed.

4.3 The following obligations apply to DSS only:

If a SP Customer is requesting Signatures with Individual Internal Identities, Service Provider must ensure that SP Customer (a) verifies the Individual's identity via face to face verification and submit accurate identity information with each Signature request for Subscribers; (b) ensures that the Individual's identity information submitted by SP Customer to request Certificates and Signatures is for a current employee or contractor of SP Customer who has consented to the request; and (c) creates and keeps records of the Identity Verification Process.

4.4 If a SP Customer is applying Electronic Seals to documents, Service Provider must ensure that SP Customer (a) only submits requests in the name of an actual department at SP Customer; (b) does not submit requests in the name of an Individual; (c) does not submit requests that are inaccurate or misleading, and (d)

agrees to the terms of the Subscriber Agreement applicable to “Subject”.

5. Termination. In addition to the termination rights in Section 7.1 of the Agreement, this Service Schedule may be terminated by GlobalSign (i) for DSS, if Adobe discontinues or GlobalSign is no longer a member of the AATL program, or (ii) for QTSeals from DSS, if the eIDAS

Regulation is discontinued or GlobalSign is no longer a member of the eIDAS trusted list. Service Provider’s failure to comply with the AATL Technical Requirements or breach of Section 4 of this Service Schedule (Service Provider DSS and QTSeals from DSS Obligations, as applicable) shall be considered a material breach of the Agreement.

Service Schedule to Partner Special Terms for Service Providers for Certificates

This Service Schedule applies only if Partner is a Service Provider AND is purchasing Certificates (as shown on the Order Summary).

1. Definitions

ACME Account: An account created when a Service Provider registers its public key with the ACME CA server that provides the ACME Service.

ACME Service: A service that supports automated certificate issuance and revocation using the ACME protocol.

Certificate API: The Service API described in the “Atlas Certificate Management API Specification” available at <https://support.globalsign.com/atlas/atlas-apis-non-portal/atlas-certificate-management-api>, as may be updated by GlobalSign from time to time.

Enterprise Registration Authority (ERA): An organization that verifies Certificate requests for Subjects within the organization.

GlobalSign Public Root: A GlobalSign Publicly Trusted root certificate that is embedded into one or more root stores of application software vendors/browsers and undergoes an annual WebTrust audit. GlobalSign Public Roots are listed in the CPS.

Privately Trusted: A Certificate that is not Publicly Trusted.

Publicly Trusted: A Certificate that is trusted by virtue of the fact that its corresponding root CA Certificate is distributed in widely available application software.

SAN License Limit: The maximum number of unique SANs across all Active Certificates that Service Provider may issue as shown on the Order Summary.

SAN License Period: The period in months starting on the Product Term Start Date as shown on the Order Summary.

Wildcard SAN Multiplier: The number of SANs that will be deducted from Service Provider’s SAN License Limit when Service Provider uses a Wildcard SAN as shown on the Order Summary. Each Wildcard SAN counts as multiple SANs within the SAN License

2. The Service

GlobalSign will provide Service Provider with access to the Service on GlobalSign’s Atlas platform for its own use and in support of SP Customers to issue Certificates for the purposes set forth in the CPS. The Service can be enabled to issue and manage Publicly Trusted and/or Privately Trusted Certificates, depending upon the Products purchased. Service Provider may request and manage Certificates using the Certificate API or ACME Service. The specific certificate life cycle management features available will depend on the method selected by Service Provider.

Use of the Certificate API or ACME Service allows Service Provider to (a) validate domains using any of the options supported by those methods; (b) request, receive and revoke Certificates; and (c) perform other queries and actions as supported by those methods.

If a SP Customer is requesting Publicly Trusted Certificates, the Certificates and Services shall be provided in accordance with the CPS which is incorporated by reference into this Agreement. Service Provider shall be considered the Subscriber/Applicant for purposes of this Agreement and must ensure that Partner and any Subjects, including but not limited to its employees or contractors, comply with the terms of the Subscriber Agreement.

3. The Products

Unless otherwise instructed by Service Provider, GlobalSign will publish Publicly Trusted TLS Certificates to Certificate Transparency (CT) logs and as required for trust by the Google Chromium Certificate Transparency Policy.

3.1 Domain Validation. For Publicly Trusted Certificates, Service Provider must confirm domain control of domain names in accordance with the Certificate API or the ACME Service (as applicable) and the CPS.

3.2 Organization Validation. For Publicly Trusted Certificates that include an Organization Validated (OV) Certificate Identity, GlobalSign will verify the organization details provided to GlobalSign by Service Provider in the

Portal to create an Organization Validated (OV) Certificate Identity for Service Provider in accordance with the applicable organization validation rules for the selected Product.

3.3 IntranetSSL Certificates. IntranetSSL Certificates are Privately Trusted Certificates issued for a SP Customer's internal use only to secure one or more FQDNs.

3.4 SAN Licensing. During the SAN License Period, Service Provider may issue Certificates that contain SANs and Wildcard SANs up to the SAN License Limit (including any Wildcard SAN Multiplier) shown in the Order Summary. Service Provider may increase the SAN License Limit by purchasing additional SAN Licenses on a pro-rated basis. If Service Provider does not renew the SAN License, GlobalSign may revoke any Active Certificates three (3) months after the end of the SAN License Period.

3.5 S/MIME Certificates. Service Provider must confirm authorization or control of the requested email domain(s) or confirm that the mailbox holder has control of the requested Mailbox Address(es) in accordance with the Certificate API or the ACME Service (as applicable) and the CPS.

Depending on the product ordered, Service Provider can request the following S/MIME Certificate types: (a) Mailbox validated: Certificate that only includes an Email Address; (b) Organization validated: Certificate for a Legal Entity; or (c) Sponsor validated: Certificate for an Individual affiliated with a Legal Entity.

4. Service Provider Obligations

4.1 Administrator role. Service Provider must appoint an Administrator to authorize and verify Certificate requests on behalf of Service Provider. The authority and assignment of this role are perpetual until revoked by Service Provider or GlobalSign.

4.2 S/MIME Certificates. For Certificate requests for Sponsor validated Certificates, SP Customer: (a) acts as an Enterprise RA and must comply with the Enterprise RA requirements outlined in Appendix A of the CPS; (b) must collect and verify Individual information (meaning a personal name or pseudonym); and (c) may only request Certificates for Individuals within the organization.

If Service Provider uses the Service for its own use, Service Provider must also comply with any obligations applicable to "SP Customer".
Service Provider's failure to comply with this Section 4.2

shall be considered a material breach of the Agreement.

5. Management of SP Customer Accounts

Service Provider may act on behalf of certain SP Customers to set up and manage the SP Customer's Organization Validated (OV) Certificate Identity and serve as the Administrator for the SP Customer's Organization Validated (OV) Certificate Identity. Service Provider may only request Certificates from a SP Customer's Organization Validated (OV) Certificate Identity that are authorized by the SP Customer for domains that have been added to the SP Customer's Organization Validated (OV) Certificate Identity. Service Provider shall only request domains to be added to the Service Provider's account when specifically authorized by the SP Customer.

For each SP Customer that Service Provider wishes to act as the agent for the SP Customer's account, Service Provider will provide GlobalSign with a Letter of Authorization (LOA) signed by the SP Customer, in a form provided by GlobalSign. Upon receipt of each LOA from Service Provider, GlobalSign will validate the authority of the signatory to sign the LOA on behalf of the SP Customer and the authenticity of the signatory's signature. Service Provider is responsible for ensuring compliance of SP Customers with the obligations applicable to "SP Customer" in this Service Schedule and the LOA.

If a SP Customer is no longer a customer of Service Provider or withdraws its authorization for Service Provider to act as an outsource provider of Certificate lifecycle management functions for the SP Customer's applicable account(s), Service Provider shall immediately notify GlobalSign in writing. GlobalSign will deactivate the SP Customer's account(s) upon (i) receipt of written request from SP Customer or Service Provider, or (ii) if GlobalSign is unable to validate the LOA as described above. Service Provider shall indemnify and hold harmless GlobalSign, its affiliates and their assigns, agents, officers, and employees harmless from and against any claims, demands, liabilities, losses, costs, damages or expenses (including reasonable attorneys' fees) arising out of or related to Service Provider's actions or inactions with respect to the creation or management of a SP Customer's account and domains or related certificate issuance or management.

6. Audit Rights. GlobalSign has the right to audit Service Provider's compliance with its obligations under Section 4.2 (S/MIME Certificates) above, upon reasonable notice,

during the Product Term and for a period of ten (10) years following any termination or expiration of the Product Term. Service Provider will provide GlobalSign and its auditors, other advisors and regulators (“Auditors”) with all reasonable cooperation, access and assistance in relation to each audit. Within five (5) days of GlobalSign’s request, Service Provider will make available the requested information. Service Provider may provide redacted or excerpted records as necessary

to comply with any applicable data privacy laws. If any audit reveals a failure of Service Provider to comply with Section 4.2 above, GlobalSign shall have the right to suspend Service Provider’s use of the Service until such time as Service Provider has remediated the non-compliance to GlobalSign’s reasonable satisfaction, and GlobalSign has confirmed that Service Provider can resume use of the Service.

Service Schedule to Partner Special Terms for Service Providers for Qualified Signing Service (QSS)

This Service Schedule applies only if Partner is a Service Provider AND is purchasing QSS (as shown on the Order Summary).

1. Definitions

Identity: A full name (including surname and given names consistent with the national identification practices) and date and place of birth, reference to a nationally recognized Identity Document, or other attributes which can be used to, as far as possible, distinguish the person from others with the same name.

Identity Validation: Verifying the Identity of the Subscriber and/or Subject.

Qualified Certificate: A Certificate that meets the requirements of a “Qualified Certificate for Electronic Signature” or “Qualified Certificate for Electronic Seal”.

Qualified Certificate for Electronic Signature: A Certificate for electronic signatures that meets the requirements laid down in Annex I of the eIDAS Regulation.

Qualified Certificate for Electronic Seal: A Certificate for an electronic seal, that meets the requirements laid down in Annex III of the eIDAS Regulation.

Subject: The natural or legal person identified in a Certificate as the subject.

2. The Service. In order to use QSS, You must complete a purchase a Product Pack, and enroll for a mTLS Certificate for connecting to the Service API.

If Certificates must include SP Customer information, You must submit SP Customer’s organization identity information for verification by GlobalSign to create the Organization Validated (OV) Certificate Identity.

There are two configuration options available for the Service: (a) Signatures for Individuals (Electronic Signatures); and (b) Signatures for the SP Customer’s Organization (Electronic Seals).

A QSS Product Pack includes Qualified Timestamps equal in number to two times the quantity of Signatures purchased in the Product Pack. Additional Qualified Timestamps may be purchased

with a QSS Product Pack or as a standalone Product Pack.

Service Provider must submit to GlobalSign a completed and signed ‘Agreement for Qualified Signing Service for Customers of Service Providers’ in a form prescribed by GlobalSign (the “SP Customer Agreement”) for each SP Customer before GlobalSign will perform the authentication steps required to create an Identity for the SP Customer under Service Provider’s account.

3. Limitations on Use

Service Provider shall not request more than five (5) Signatures per second or more than one (1) Certificate per second.

Service Provider may not request more than the number of timestamps purchased in a Product Pack. Service Provider shall not request more than five (5) Qualified Timestamps per second. Service Provider shall be responsible for applying any timestamps into the documents. Service Provider shall maintain the confidentiality of the URL and not share it with third parties.

The pairing of the Signer’s account and his/her mobile device will require confirmation of two PINs, one sent to the Signer’s phone number and one sent to the Signer’s email address provided by Service Provider using an Application made available to the Signer in certain third party App stores (the “QSS App”). Use of the QSS App is governed by separate terms and conditions agreed by the Signer at the time the QSS App is downloaded. Service Provider and Signer must ensure that the PINs are requested judiciously and with appropriate gaps to account for communication delays and avoid abuse of the feature.

4. Service Provider Obligations

Service Provider is responsible for ensuring compliance of SP Customers with the obligations applicable to “SP Customer” in this Service Schedule and the SP Customer Agreement. If Service Provider uses the Service for its own use,

Service Provider must also comply with any obligations applicable to "SP Customer".

GlobalSign reserves the right to require changes to a SP Customer's process for Identity Validation based on changes to the regulatory or compliance requirements, upon request of the GlobalSign's auditors or supervising authorities or for other reasons as may be reasonably required by GlobalSign to ensure the proper functioning and reliability of the Service. GlobalSign will inform You of expected changes with reasonable notice. SP Customer must promptly implement any requested changes or immediately cease use of the Service if requested by GlobalSign.

4.1 Service Provider shall: (a) ensure all key activations and key pairs are controlled by the Subject and the Subject must be authenticated for accessing Subject's account; (b) ensure that information provided on the enrollment requests is complete and accurate; (c) be solely responsible for developing or integrating the digitally signed hash and timestamp into Service Provider's document management system by either using the Service API or software developer kit (SDK) or configuring the Service for Service Provider's own document workflow integration; (d) confirm with the Subject that the information is correct before approving a Certificate request; and (e) request revocation of a Certificate when any information related to the Certificate request has changed.

Service Provider shall notify GlobalSign in the following cases: (i) the Identity Validation shall not be relied upon; (ii) there is a material change in the information contained in an issued Certificate; (iii) the original Certificate request was not authorized by the Subject or the Subscriber and the Subject does not retroactively grant authorization; or (iv) the Certificate is misused.

4.2 Service Provider must complete a questionnaire about its security practices in a form prescribed by GlobalSign. The provisioning of the Service to Service Provider is conditioned upon GlobalSign's approval, at GlobalSign's sole discretion, of Service Provider's questionnaire.

If SP Customer requests Certificates for its

employees, SP Customer will act as a Local Registration Authority (LRA) as governed by the "Agreement for Qualified Signing Service for Customers of Service Providers".

5. Service Suspension. Service Provider must notify GlobalSign, in writing, within seven (7) days of becoming aware of any suspected failure of Service Provider to comply with obligations in the Agreement or this Service Schedule. For Service Provider's failure to comply with obligations of Section 4 of this Service Schedule, Service Provider must notify GlobalSign within twenty-four (24) hours.

In such case, Service Provider will immediately cease the use of the Service, and GlobalSign has the right to suspend Service Provider's use of the Service.

Service Provider will promptly remediate the non-compliance and provide evidence of the remediation for review by GlobalSign. Service Provider will not resume the use of the Service until GlobalSign has reviewed the remediation and has confirmed to Service Provider that the use of the Service may be resumed.

6. Right to Audit. GlobalSign has the right to audit Service Provider's compliance with its obligations, upon reasonable notice, during the QSS Product Term and for a period of 10 years following any termination or expiration of the QSS Product Term.

Service Provider will provide GlobalSign (and its auditors, other advisors and regulators) with all reasonable co-operation, access and assistance in relation to each audit. Within five (5) days of GlobalSign's request, Service Provider will make available the requested information. Service Provider may provide redacted or excerpted records as necessary to comply with any applicable data privacy laws.

7. Termination. In addition to the termination rights in Section 7.1 of the Agreement, this Service Schedule may be terminated by GlobalSign if the eIDAS Regulation is discontinued or GlobalSign is no longer a member of the eIDAS trusted list.