Service Provider Agreement

THESE TERMS TOGETHER WITH THE APPLICABLE SERVICE SCHEDULE(S) (THE "AGREEMENT") GOVERN YOUR USE OF THE PRODUCTS AND SERVICES PURCHASED BY YOU UNDER ONE OR MORE ORDER SUMMARIES. YOU MUST READ THIS AGREEMENT CAREFULLY BEFORE USING THE SERVICE TO ACQUIRE PRODUCTS OR SERVICES. BY CHECKING THE ACCEPTANCE BOX AND PLACING YOUR ORDER, 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 ACCESS OR USE THE SERVICES OR ACQUIRE PRODUCTS.

BY CHECKING THE ACCEPTANCE BOX, YOU REPRESENT AND WARRANT THAT YOU ARE DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON BEHALF OF THE COMPANY SHOWN IN THE 'SOLD TO' FIELD ON THE ORDER SUMMARY ("SERVICE PROVIDER" OR "YOU") AND TO BIND SERVICE PROVIDER TO THE TERMS OF THIS AGREEMENT WITH GLOBALSIGN.

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.

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

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

Atlas Account: The account created by Service Provider in Atlas when using the Portal.

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

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

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.

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) and eIDAS (UK Legislation) and The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (United Kingdom).

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.

GlobalSign: The GlobalSign entity identified on the Order Summary.

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.

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.

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 without limitation, the eIDAS Regulation.

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.

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

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.

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.

Privately Trusted: A Certificate that is not Publicly Trusted.

Product: The product(s) purchased by Service Provider shown on the Order Summary, including but not limited to, Signatures, Transactions, Certificates, timestamps and OV Certificate Identities. "Product" also includes any optional add-on features or items that may be purchased by Service Provider.

Product Pack: The Products that may be ordered via Service Provider's Service, up to the value of the Quota, and available for use by Service Provider during the Product Term. Products within a Product Pack may have the same or different features.

Product Term: The period in months shown on the Order Summary.

Product Term Start Date: The date shown on the Order Summary when the Product Term begins.

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.

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

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

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

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.

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

Signature: An Electronic Signature or Electronic Seal.

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.

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.

Test Service: An instance of a Service or features made available for Service Provider's use solely for evaluation or trial purposes, including proofs of concept, beta or other testing.

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.

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.

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

2. Use of the Services and Portal. GlobalSign hereby grants to Service Provider the right to use the Services, Products and related documentation in accordance with the terms of this Agreement and the applicable Service Schedule(s).

GlobalSign hereby 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 Customers and Service Provider's own use. If Service Provider uses the Services for its own use, Service Provider must comply with all obligations applicable to "Customer" in this Agreement.

2.1 Use of the Portal. In connection with the Services, Service Provider will have access to the Portal after Service Provider's creation of an Atlas Account. In the Portal, Service Provider may perform functions such as purchasing Products, accepting sales quotes, requesting identities, and obtaining Service Credentials. GlobalSign provides Service Provider with access to the Portal. The Portal may also provide certain communications from GlobalSign, such as service announcements and other messages.   Service Provider is responsible for maintaining the confidentiality of its Service Credentials and is fully responsible for all activities that occur under Service Provider's Atlas Account. Service Provider agrees to (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 Service Provider logs out from its Atlas Account at the end of each session. GlobalSign may deactivate or remove Service Provider's Atlas Account and/or access to the Portal if Service Provider has not conducted any transactions for one (1) year or more.

2.2 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) 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 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. Limitations on Use. Service Provider 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 provided in the Agreement and the Service Schedule(s); (c) disassemble, decompile, reverse engineer or otherwise attempt to discover the source code of the 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 other than in accordance with this Agreement and in compliance with all applicable Industry Standards, laws and regulations. In addition to any specific use limitations that may be set forth in a Service Schedule, GlobalSign may set and enforce limits for reasonable use in order to prevent abuse of or undue burden on the Services.

4. CPS and Subscriber Agreement. If a Customer is requesting Publicly Trusted Certificates, (a) the Certificates and Services shall be provided in accordance with the CPS which is incorporated by reference into this Agreement and (b) Service Provider shall be considered the Subscriber/Applicant for purposes of this Agreement and must ensure that Service Provider and any of its employees or contractors comply with the terms of the Subscriber Agreement.

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

5. Test Service. The terms of this Section 5 apply if Service Provider is granted the right to access or use a Test Service.

5.1 Use Rights. Service Provider may only access or use a Test Service provided for trial purposes in a non-production, test environment, and solely for the purpose of Service Provider's internal evaluation and interoperability testing of a Service.

5.2 Test Service Period. Service Provider's right to use a Test Service will terminate immediately upon the earlier of (a) the date the number of Signatures, timestamps or Certificates in the Test Service is depleted, (b) the expiration date of the Test Service period, or (c) the date when GlobalSign terminates Service Provider's right to use a Test Service (which GlobalSign may do at any time in its sole discretion).

5.3 Warranty Disclaimer. SERVICE PROVIDER ACKNOWLEDGES THAT ANY TEST SERVICES OR PRODUCTS PROVIDED FOR EVALUATION OR TEST PURPOSES 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 SERVICES, PRODUCTS, SERVICE PROVIDER'S USE OR ANY INABILITY TO USE THE TEST SERVICES OR PRODUCTS, THE RESULTS OF ITS USE AND THIS AGREEMENT.

5.4 LIMITATION OF LIABILITY. GLOBALSIGN SHALL NOT BE LIABLE TO SERVICE PROVIDER 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 PRODUCTS OR TEST SERVICES FOR EVALUATION OR TEST PURPOSES AND THE USE OR FAILURE OF THE TEST SERVICES 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; Overage. 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 Service Provider wishes to continue to use a Service after the end of the Product Term, or if Service Provider exceeded its Quota, Service Provider may order a new Product Pack or order Products

individually. If Service Provider continues to order Products individually, the fee for each Product will be the Product Pack Overage rate shown on the Order Summary.   GlobalSign reserves the right to adjust Overage rates at any time following two (2) years after the Product Term Start Date.

6.2 Fees; Payment. Service Provider agrees to pay GlobalSign the fees for the Products and/or Services shown in the Order Summary.

On each Product Term Start Date, Service Provider shall provide to GlobalSign valid, up-to-date and complete credit card details or, if applicable, purchase order information acceptable to GlobalSign. If Service Provider provides its credit card details to GlobalSign, Service Provider hereby authorizes GlobalSign to bill such credit card for the fees payable on the Product Term Start Date for any Products ordered. If Service Provider provides its approved purchase order information to GlobalSign, and/or opts to pay by invoice, GlobalSign shall invoice Service Provider on the Product Term Start Date for the fees payable in respect of any Products ordered. If Service Provider orders a new Product Pack, GlobalSign will invoice Service Provider on the new Product Term Start Date. If Service Provider continues to order Products individually, GlobalSign will invoice Service Provider on a monthly basis in arrears at the Overage rates shown for the applicable Product on the Order Summary.

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 GlobalSign's invoices. Service Provider 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 Service Provider.

If any undisputed invoiced amount is not received by GlobalSign by the due date, then without limiting GlobalSign's rights or remedies, (a) 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, and (b) GlobalSign may suspend or limit Service Provider's access to the Portal or Service without notice until full payment is made. Service Provider 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 Order Date of the first Order Summary (the "Effective Date") and will continue unless terminated earlier as provided herein.

7.1 Termination of Agreement. *By Service Provider*: This Agreement or any Service Schedule may be terminated by Service Provider at any time upon no less than thirty (30) days' written notice to GlobalSign. *By GlobalSign*: This Agreement or any Service Schedule may be terminated by GlobalSign upon written notice to Service Provider (a) if Service Provider materially breaches this Agreement and such breach continues for a period of thirty (30) days after notice thereof has been given by GlobalSign; (b) if Service Provider files for bankruptcy, ceases to carry on business, or undergoes liquidation; (c) if Service Provider 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; or (d) at any time upon no less than ninety (90) days' written notice to Service Provider. *By either party*: Either party may terminate this Agreement or any Service Schedule immediately upon written notice if the other party is in breach of Section 10 (Confidentiality) of this Agreement.

8.   Effect of Termination. Upon termination or expiration of this Agreement or Service schedule, (1) Service Provider and Customers shall discontinue use of the applicable Services, (2) all rights and obligations of the parties under this Agreement or Service Schedule shall cease immediately except the terms and conditions of this Agreement and any applicable Service Schedule shall continue to apply to any Products issued and/or used prior to the termination until the expiration or earlier revocation of the applicable Product, and (3) GlobalSign will refund any unused fees if terminated by GlobalSign under 7.1(d) above. The following Sections shall survive any expiration or termination of this MSA: 1, 6, 7 and 9 – 16.

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

9.4 Personal Data. Service Provider warrants that (i) it has the necessary rights to provide any personal data or other information that Service Provider 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 Service Provider and Customer Personal Data, as defined in the DPA.

9.5 No Other Warranty**.** EXCEPT AS PROVIDED IN THE CPS OR TPS AT https://www.globalsign.com/en/repository, AND 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, 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 the 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 Receiving Party's obligations with respect to Confidential Information will expire three (3) years after the termination of this Agreement.

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; or (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.

11. Ownership. Except for the rights expressly granted under this Agreement, all right, title and interest in and to the Service, Products, APIs, and Portal is 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.

12. Indemnification

12.1 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 use of the Services by Service Provider as permitted hereunder infringes upon any copyright, trademark, trade secret, United States or European patent or other intellectual property right of any third party.

12.2 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.

12.3 Service Provider 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 Service Provider accessed or used the Customer's account without authorization from the Customer, outside of the scope of its authority or in contravention of instructions given by the Customer, (ii) breach of this Agreement by Service Provider, (iii) purchase or use of the Service or Products by a third party who is accessing or acquiring the Service or Product through Service Provider, (iv) use of any Third Party Products in combination with the Service, or (v) Service Provider's failure to comply with Section 2.1 above.

12.4 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 Service Provider 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 Service Provider for the Services, including the applicable Products, 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 Service Provider 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 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	London, England
GlobalSign NV	Belgium	Leuven, Belgium
GMO GlobalSign, Inc. (US)	New Hampshire,	State and federal courts of New Hampshire
GMO GlobalSign Pte. Ltd	Singapore	Singapore
GMO GlobalSign Inc.	Philippines	Makati City, Philippines
GMO GlobalSign Certificate Services Pvt. Ltd	Laws of Republic	Delhi, India
GMO GlobalSign Russia LLC	Russia Federation	Moscow, Russia
GMO GlobalSign Solutions in Technology	Brazil	Belo Horizonte, Brazil
GMO GlobalSign FZ LLC	United Arab	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; 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 hand delivery, regular mail, or overnight courier service to GlobalSign - the GlobalSign address and Service Provider - the "Sold To" address shown in the Order Summary. 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 below 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 Service Provider 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 MSA 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.

17. Entire Agreement. This Agreement, Service Schedules and any documents incorporated herein by reference constitute the entire agreement between the parties and supersedes 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 Service Provider's general terms and conditions contained in any purchase order or other document issued by Service Provider. 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 Service Provider, the order of precedence shall be: the Order Summary, this Agreement, the Subscriber Agreement, CPS and TPS.

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). If such an amendment materially and adversely affects Service Provider's rights herein, Service Provider will have the right, as its sole and exclusive remedy in connection with such amendment, to terminate this Agreement during the 30-day period after GlobalSign's notice of such amendment, by providing written notice of termination to GlobalSign. Service Provider's continued use of the Service after 30 days of GlobalSign's notice of the amendment constitutes Service Provider's acceptance of the amendment.

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.

[Service Provider Agreement v 1.6 February 15, 2023]

Service Schedule for Digital Signing Service (DSS) and Timestamps

This Service Schedule applies only if Service Provider is purchasing DSS or timestamps (as shown on the Order Summary) or Digital Signature Transactions using GMO Sign. Other capitalized terms used in this Service Schedule have the meaning set forth elsewhere in the Agreement.

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.

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.

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 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 Customer's Organization Validated (OV) Certificate Identity.

SEIKO Timestamp: An RFC3161 compliant timestamp

accredited by the Government of Japan and provided by SEIKO.

Trusted Third Party: A third party approved by GlobalSign that maintains a secure process used by 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 Customer's organization identity information for verification by GlobalSign to create the 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, 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, Customer's Identity Verification Process in order to comply with the AATL Technical Requirements. Service Provider shall require that Customer promptly implements any requested changes or immediately ceases use of DSS if requested by GlobalSign.

2.2 Timestamps

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

2.3 Qualified Timestamps

If Service Provider purchases a Product Pack for 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. The TPS available at http://www.globalsign.com/repository/ is incorporated by reference into this Service Schedule.

3. Limitations on Use

Service Provider shall not request more than five (5) Signatures per second or the creation of more than five (5) Individual Identities or Electronic Seals every five (5) seconds unless Service Provider has purchased a higher rate limit. 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 QTSA timestamps per second or one (1) SEIKO timestamp per second. Service Provider or its 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 Customers.

4. Service Provider DSS Obligations

4.1 If a 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 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; (f) request revocation of a Certificate when any information related to the Certificate request has changed; and (g) ensure compliance by each Individual Subscriber with the terms of the Subscriber Agreement.

4.3 If a Customer is requesting Signatures with Individual Internal Identities, Service Provider must ensure that 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 Customer to request Certificates and Signatures is for a current employee or contractor of Customer who has consented to the request; and (c) creates and keeps records of the Identity Verification Process.

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

5. Fees

There is an additional charge for Qualified Timestamps and any additional OV Certificate Identities.

6. Termination. In addition to the termination rights in Section 7.1 of the Agreement, this Service Schedule may be terminated by GlobalSign if Adobe discontinues or GlobalSign is no longer a member of the AATL program. Service Provider's failure to comply with the AATL Technical Requirements or breach of Section 4 of this Service Schedule (Service Provider DSS Obligations) shall be considered a material breach of the Agreement.

Service Schedule for Certificates

This Service Schedule applies only if Service Provider is purchasing Certificates (as shown on the Order Summary). Other capitalized terms used in this Service Schedule have the meaning set out elsewhere in the Agreement.

1. Definitions

ACME Account: An account created when a Customer 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.

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 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 GlobalSign 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.

3. The Products

Unless otherwise instructed by Service Provider, GlobalSign will publish Publicly Trusted SSL/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 TLS and S/MIME Certificates, Service Provider must validate 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 Customer's internal use only to secure one or more FQDNs.

4. Service Provider Obligations

Service Provider warrants that Service Provider (a) has the right to hold the private key corresponding to the public key listed in any Certificates, (b) has taken, and will take, all appropriate, reasonable, and necessary steps to maintain control of, secure, properly protect and keep secret and confidential the private key corresponding to the public key in the Certificates, and (c) will maintain sole control of the private key.

5. Management of Customer Accounts

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

For each Customer that Service Provider wishes to act as the agent for the Customer's account, Service Provider will provide GlobalSign with a Letter of Authorization (LOA) signed by the Customer, in a form provided by GlobalSign. Service Provider must provide a new signed

LOA from the Customer at least every eleven (11) months. Upon receipt of each LOA from Service Provider, GlobalSign will validate the authority of the signatory to sign the LOA on behalf of the Customer and the authenticity of the signatory's signature.

If a Customer is no longer a customer of Service Provider or withdraws its authorization for Service Provider to on behalf of the Customer's for the applicable account(s), Service Provider shall immediately notify GlobalSign in writing. GlobalSign will deactivate the applicable Customer's account(s) upon (i) receipt of written request from Customer or Service Provider, (ii) Service Provider's failure to provide a new signed LOA from the applicable Customer after 12 months, or (iii) 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 Customer's account and domains or related certificate issuance or management.

Service Schedule for Qualified Signing Service (QSS)

This Service Schedule applies only if Service Provider is purchasing QSS (as shown on the Order Summary). Other capitalized terms used in this Service Schedule have the meaning set out elsewhere in the Agreement.

1. Definitions

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.

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 Customer information, You must submit 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 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 "Customer Agreement") for each Customer before GlobalSign will perform the authentication steps required to create an Identity for the 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 Customers with the obligations applicable to "Customer" in this Service Schedule and the Customer Agreement.

If Service Provider uses the Service for its own use, Service Provider must also comply with any obligations

applicable to "Customer".

GlobalSign reserves the right to require changes to a 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. 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.

Service Provider agrees to the terms of the Subscriber Agreement applicable to "Subscriber".

Use of Timestamps must comply with the CPS and TPS.

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 Customer will request Certificates for its employees, 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 MSA or this Service Schedule. For Service Provider's failure to comply with obligations of Section 4 (**Error! Reference source not found.**) 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.