Master Services Agreement

THIS MASTER SERVICES AGREEMENT (THE “MSA”) AND APPLICABLE SERVICE SCHEDULE(S) GOVERN YOUR USE OF THE PRODUCTS AND SERVICE(S) PURCHASED BY YOU UNDER ONE OR MORE ORDER SUMMARIES. YOU MUST READ THIS MSA CAREFULLY BEFORE PURCHASING PRODUCTS OR SERVICES. BY CHECKING THE ACCEPTANCE BOX AND PLACING YOUR ORDER, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS MSA. IF YOU DO NOT AGREE TO THE TERMS OF THIS MSA, YOU WILL NOT BE PERMITTED TO ACCESS OR USE A SERVICE OR ANY PRODUCTS.

BY CHECKING THE ACCEPTANCE BOX, YOU REPRESENT AND WARRANT THAT YOU ARE AUTHORIZED TO ACCEPT THIS MSA ON BEHALF OF THE COMPANY SHOWN IN THE ‘SOLD TO’ FIELD ON THE ORDER SUMMARY ("COMPANY", “CUSTOMER” OR “YOU”) AND TO BIND COMPANY TO THE TERMS OF THIS MSA WITH GLOBALSIGN.

1. Definitions

ACME MAC Key: An authentication code used for ACME external account binding between Customer’s ACME Account and Customer’s Atlas Account.

Administrator: A user registered in Customer’s Atlas Account and who has access to perform functions on behalf of Customer.

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 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 Customer 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 Customer in Atlas when using 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.

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).

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.

FlexQuota: The per unit price for a Product paid when Customer 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 entity identified on the Order Summary. Notwithstanding the foregoing, if a Subscriber orders an eIDAS Qualified Certificate “GlobalSign” shall mean GlobalSign NV (Belgium).

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 regulatory or quasi-regulatory standards, including but not limited to, the eIDAS Regulation.

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

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

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

Product Pack: The Products that may be ordered via Customer's Services, up to the value of the Quota, and available for use by Customer 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 when the Product Term begins. The Product Term Start Date is the date when the Service is activated unless the Order Summary includes a Custom CA. If the Order Summary includes a Custom CA, the Product Term Start Date is the date when the Service becomes available on the date of the key ceremony.

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 Customer as shown on an Order Summary.

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

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

Service Schedule: The additional terms and conditions applicable to specific Products or Services ordered by Customer.

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.

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.

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

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 may be used 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.

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

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

2. Use of the Services and Portal. GlobalSign hereby grants to Customer the right to use the Services, Products and related documentation for enterprise use in accordance with the terms of this MSA and the applicable Service Schedule(s). If Customer has purchased Premium support, for the Product Term GlobalSign shall provide the services in the GlobalSign Service and Support SLA available at https://media.globalsign.com/GlobalSign_Service_and_Support_Service_Level_Agreement.

GlobalSign hereby grants to Customer a non-exclusive, non-transferable, non-sublicensable, revocable license during the term of this MSA to use and make calls to/from a Service API solely for the purpose of facilitating Customer's use of a Service.

2.1 Use of the Portal. In connection with the Services, Customer will have access to the Portal after Customer's creation of an Atlas Account. In the Portal, Customer's Administrators may perform functions such as purchasing Products, accepting sales quotes, requesting identities, and obtaining Service Credentials. The Portal may also provide certain communications from GlobalSign, such as service announcements and other messages. Customer is responsible for maintaining the confidentiality of its Service Credentials held by Customer and is fully responsible for all activities that occur under Customer's Atlas Account. Customer 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 Customer logs out from its Atlas Account at the end of each session. GlobalSign may deactivate or remove Customer's Atlas Account and/or access to the Portal if Customer 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 Customer. Customer'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 Customer 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 Customer Confidential Information, including but not limited to, any Service Credentials, Customer hereby authorizes GlobalSign to allow the third party to access Customer Confidential Information as necessary for interoperation. Customer agrees that GlobalSign shall have no responsibility or liability to Customer 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. Customer 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 this MSA 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 MSA 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, TPS and Subscriber Agreement. If 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 MSA, and (b) Customer shall be considered the Subscriber/Applicant for purposes of this MSA and must ensure that Customer and any Subjects, including but not limited to its employees or contractors, comply with the terms of the Subscriber Agreement. Use of Certificates must comply with the Subscriber Agreement and CPS. Use of Timestamps must comply with the CPS and TPS.

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

5.1 Trial Products. Customer may use Trial Products solely for the purpose of its evaluation of a Product. Customer'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 Customer's right to use the Trial Products (which GlobalSign may do at any time in its sole discretion).

5.2 Test Products. Customer may only use a Test Product for test purposes in a non-production, test environment, and solely for the purpose of Customer's internal evaluation and interoperability testing of a Service. Customer'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 Customer'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. CUSTOMER 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, CUSTOMER'S USE OR ANY INABILITY TO USE TEST OR TRIAL PRODUCTS, THE RESULTS OF THEIR USE AND THIS MSA.

5.4 LIMITATION OF LIABILITY FOR TEST OR TRIAL PRODUCTS. GLOBALSIGN SHALL NOT BE LIABLE TO CUSTOMER 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 TRIAL OR TEST PRODUCTS AND THE USE OR FAILURE OF THE TRIAL OR TEST PRODUCTS TO OPERATE FOR WHATEVER REASON, WHETHER SUCH ACTION IS BASED IN CONTRACT OR TORT OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, NEGLIGENCE.

6. Product Packs; Fees; Payment

6.1 Product Packs; FlexQuota. Product Packs expire at the end of the Product Term. There is no credit or refund for unused Products in a Product Pack. If Customer wishes to continue to use a Service or Products after the end of the Product Term, or if Customer exceeds its Quota, Customer may order a new Product Pack or Service 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. Customer agrees to pay GlobalSign the fees for the Products and/or Services shown in any Order Summary.

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

GlobalSign will invoice/charge Customer (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 Customer or charge Customer's credit card (as applicable) for any recurring fees in accordance with the billing frequency shown on the Order Summary.

If Customer orders Products individually (whether after the end of the Product Term or on a pay-as-you-go basis), GlobalSign will invoice/charge Customer on a monthly basis in arrears at the FlexQuota price shown for the 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 Services and Products are exclusive of any and all taxes or duties. Such taxes and duties, when applicable, will be added to the invoices. Customer will pay any taxes, fees and similar governmental charges related to the execution or performance of this MSA, other than applicable income taxes imposed on GlobalSign related to its receipt of payments from Customer.

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 Customer's access to the Portal or Services without notice until full payment is made. Customer 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 MSA begins on the Order Date of the first Order Summary (the "Effective Date") and will continue unless terminated earlier as provided herein. The term of a Service Schedule begins on the Order Date and will continue until the applicable Service Schedule is terminated as provided herein.

7.1 Termination; Non-Renewal.

7.1.1 By Customer: This MSA or any Service Schedule may be terminated by Customer at any time upon no less than thirty (30) days' written notice to GlobalSign. Notwithstanding the foregoing, if the Order Summary includes Annual Products, any termination for convenience will not be effective until the end of the then current Product Term. Annual Products will renew automatically on the same terms and conditions for successive Product Terms of twelve (12) months unless either party gives the other party notice of its intention not to renew the Annual Products at least thirty (30) days prior to the end of the then current Product Term. Customer can provide such notice by sending an email to its local sales office referencing the relevant Order ID.

7.1.2 *By GlobalSign*: This MSA or any Service Schedule may be terminated by GlobalSign upon written notice to Customer: (a) if Customer materially breaches this MSA or any Service Schedule and such breach continues for a period of thirty (30) days after notice thereof has been given by GlobalSign; (b) if Customer files for bankruptcy, ceases to carry on business, or undergoes liquidation; (c) if Customer is unable to perform a material portion of its obligations under this MSA 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 Customer. Notwithstanding the foregoing, this MSA may be terminated immediately by GlobalSign upon written notice if GlobalSign determines, in its reasonable discretion, that

Customer poses a security or compliance risk to the Service or GlobalSign.
7.1.3 *By either party*: Either party may terminate this MSA or any Service Schedule immediately upon written notice if the other party is in breach of Section 10 (Confidentiality).

8. Effect of Termination. Upon termination or expiration of this MSA or a Service Schedules, (1) Customer shall discontinue use of the applicable Services, (2) all rights and obligations of the parties under this MSA or Service Schedule shall cease immediately except the terms and conditions of this MSA 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, (3) GlobalSign will cease providing validation services for any Customer Private Root CAs and ICAs, i.e. OCSP or CRL and immediately revoke all Certificates and issuing CAs unless Customer requests continuation of validation services and pays the applicable annual hosting fees, and (4) GlobalSign will refund any unused fees if terminated by GlobalSign under 7.1.2(d) above. The following Sections shall survive any expiration or termination of this MSA: 1, 6, 7 and 9 – 16 of this MSA and any applicable "Audit Rights" in a 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 MSA and that this MSA has been duly executed and delivered by such party and constitutes the valid and binding obligation of such party.

9.3 Subscriber Information. Customer warrants that all information and representations made by the Subscriber are true.

9.4 Personal Data. Customer warrants that (i) it has the necessary rights to provide any personal data or other information that Customer 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.pdf ("DPA") are hereby incorporated by reference and shall apply to the extent GlobalSign processes any Customer or 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, 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 this MSA. 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; or (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 MSA, 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. Except for the rights expressly granted under this MSA, 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 Services and all other products, software, documentation, works, and other intellectual property created, used, or provided by GlobalSign for the purposes of this MSA, 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 Customer against any cost, loss or damage from any claim, demand, suit or action brought by a third party against Customer alleging that use of the Services by Customer 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 Customer, the right for Customer to continue using the Services as contemplated hereunder; (b) modify the Service, 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 MSA.

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 Customer, or (ii) the combination of the Services with items not supplied by GlobalSign, including any Third Party Products.

12.3 Customer 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) breach of this MSA by Customer, (ii) use of the Service or Products by a third party who is accessing or acquiring the Service or Products through Customer, (iii) use of any Third Party Products in combination with the Service, or (iv) Customer'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 Customer for any and all claims arising out of or relating to this MSA, or the use of or inability to use the Services or Products, will in no event exceed the amount of fees paid by Customer 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 Customer 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 MSA 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 MSA 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 Hampshire
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; 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 MSA.

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 Customer's "Sold To" address on the Order Summary

or (ii) email to GlobalSign to legal@globalsign.com and to Customer to the email for Customer's main contact in Customer'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 MSA shall be binding upon, and inure to the benefit of, the successors, executors, heirs, representatives, administrators and assigns of the parties hereto. This MSA may not be transferred or assigned by Customer 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 MSA.

16.4 Severability. If and to the extent that any court holds any provision of this MSA to be unenforceable, such unenforceable provision shall be stricken and the remainder of this MSA shall not be affected thereby. The parties shall in good faith attempt to replace any unenforceable provision of this MSA 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 MSA, 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 MSA (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 Customer's general terms and conditions contained in any purchase order or other document issued by Customer. In the event of any conflict between the terms of the Order Summary, this MSA, the Subscriber Agreement, CPS, TPS, and the terms of any purchase order or any other document issued by Customer, the order of precedence shall be: the Order Summary, this MSA, 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 Customer's rights herein, Customer will have the right, as its sole and exclusive remedy in connection with such amendment, to terminate this MSA during the 30-day period after GlobalSign's notice of such amendment, by providing written notice of termination to GlobalSign. Customer's continued use of the Service after 30 days of GlobalSign's notice of the amendment constitutes Customer's acceptance of the amendment.

19. Language. This MSA is drafted in the English language. Any notice given under or in connection with this MSA shall be in English. All other documents provided under or in connection with this MSA shall be in English or accompanied by a certified English translation. The English language version of this MSA and any notice or other document relating to this MSA shall prevail if there is a conflict.

20. Third Party Beneficiaries. This MSA benefits solely the parties to this MSA and their respective permitted successors and assigns and nothing in this MSA, 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 MSA.

Service Schedule for Digital Signing Service (DSS), Qualified Trust Seals from DSS and Timestamps

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

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 process) 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.

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 Trust Seal (QTSeals): 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.

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, You must (i) submit Customer's organization identity information for verification by GlobalSign to create the OV Certificate Identity, (ii) purchase a Product Pack, and (iii) enroll for a mTLS Certificate if Customer is integrating its application directly to the DSS API. There are three Signature configuration options available for the Service: (a) Signatures for Individual Internal Identities; (b) Signatures for Individual External Identities (via offline process); 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. Customer must promptly implement any requested changes or immediately cease 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 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 Customer 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 Customer has purchased a higher rate limit, Customer 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) seconds unless Customer has purchased a higher rate limit, or (iii) the creation of more than one QTSeal every five (5) seconds. If Customer 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.

Customer may not request more than the number of timestamps purchased in a Product Pack. Customer shall not request more than five (5) AATL or Qualified timestamps per second or one (1) SEIKO timestamp per second. Customer shall be responsible for applying any timestamps into the documents or code using the URL provided by GlobalSign. Customer shall maintain the confidentiality of the URL and not share it with any third parties.

4. DSS and QTSeals from 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 The following obligations apply to DSS and QTSeals from DSS except for 4.2 (d) and (e) which do not apply to QTSeals from DSS.

Customer 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 Customer's document management system by either using the DSS API or software developer kit (SDK) or configuring DSS for Customer'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 Customer is requesting Signatures with Individual Internal Identities, Customer must (a) verify the Individual's identity via face to face verification and submit accurate identity information with each Signature request for Subscribers; (b) ensure 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) create and keep records of the Identity Verification Process.

For each Certificate for an Individual, Customer shall ensure that the Individual accepts and complies with the terms of the Subscriber Agreement applicable to "Subject".

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

Customer 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 MSA, 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. Customer's failure to comply with the AATL Technical Requirements or breach of Section 4 of this Service Schedule (DSS and QTSeals from DSS Obligations, as applicable) shall be considered a material breach of the MSA.

Service Schedule for Certificates

This Service Schedule applies only if Customer is purchasing Certificates (as shown on the Order Summary).

1. Definitions

ACME Account: An account created when 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.

Active Certificate: A Certificate that is not expired or revoked.

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.

SAN License Limit: The maximum number of unique SANs across all Active Certificates that Customer 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 Customer's SAN License Limit when Customer 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 Customer with access to the Service on GlobalSign's Atlas platform for enterprise use only 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. Customer 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 Customer.

Use of the Certificate API or ACME Service allows Customer 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 Customer, 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 Certificates Customer 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 by Customer in the Portal to create an Organization Validated (OV) Certificate Identity for Customer in accordance with the applicable organization validation rules for the selected Product.

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

3.4 SAN Licensing. During the SAN License Period, Customer 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. Customer may increase the SAN License Limit by purchasing additional SAN Licenses on a pro-rated basis. If Customer 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. Customer 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, Customer 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. Customer Obligations

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

4.2 S/MIME Certificates. For Certificate requests for Sponsor validated Certificates, 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. Customer's failure to comply with this Section shall be considered a material breach of the MSA.

5. Audit Rights. GlobalSign has the right to audit Customer'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. Customer 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, Customer will make available the requested information. Customer may provide redacted or excerpted records as necessary to comply with any applicable data privacy laws. If any audit reveals a failure of Customer to comply with Section 4.2 above, GlobalSign shall have the right to suspend Customer's use of the Service until such time as Customer has remediated the non-compliance to GlobalSign's reasonable satisfaction, and GlobalSign has confirmed that Customer can resume use of the Service.

Service Schedule for GMO Sign

This Service Schedule applies only if Customer is purchasing GMO Sign (as shown on the Order Summary). If Customer is purchasing Digital Signature Transactions, the terms of the 'DSS and Timestamps Service Schedule' also apply.

1. Definitions

Digital Signature (D-Sign) Transaction: Each document sent by a user requesting Digital Signature, when a user is the sender of a request for Digital Signature, regardless of the number of Signatures requested or applied to the document by other internal users; and/or each Digital Signature applied to a document by a user when a user is the recipient of a request for Digital Signature from an external user.

Electronic Signature (E-Sign) Transaction: Each document sent by a Customer internal user requesting Electronic Signature, regardless of the number of Signatures requested or applied to the document.

2. Service. GMO Sign is a cloud-based signing service that helps customers sign and manage electronic documents using Electronic Signatures or Digital Signatures (using DSS).

The GMO Sign Help Center offers articles to help you understand various features of GMO Sign and how those features work. Customer is expected to check these articles at https://gmo-agree.zendesk.com/hc/en-us for any functional support. Customer may also raise a request for help with any technical issue at support-gmosign@globalsign.com.

GlobalSign may, without notice to Customer, at the discretion of GlobalSign, temporarily suspend or interrupt GMO Sign in order to conduct maintenance and other administrative work.

GlobalSign is not responsible for performing any backups of any data or documents for Customer. Customer is solely responsible for taking appropriate measures to back up its data and documents.

3. Customer Obligations. Customer must provide accurate identity information for each user at the time of user registration. If there is any change in the information Customer provided to GlobalSign when applying for GMO Sign, you must immediately notify GlobalSign of such change by contacting your GlobalSign account manager. No change is considered effective until GlobalSign confirms receipt of the notification.

4. Limitations on Use. Customer may not use GMO Sign in China or Russia unless authorized by GlobalSign in the form of an amendment to the MSA.

5. Compliance with Laws. Customer is responsible for determining how long to retain any contracts, documents, and other records under any applicable laws or regulations, or its own business policies. Further, Customer is solely responsible for determining the suitability of GMO Sign for Customer's business and complying with any applicable data privacy and protection regulations, laws or conventions applicable to Customer data and Customer's use of GMO Sign.

GlobalSign has no responsibility with regard to the contents of any electronic contract concluded using GMO Sign and does not make any warranty that a person with legitimate authority signed an electronic contract using the Service.

Electronic signing of certain types of agreements and documents may not be permitted under local electronic signature laws or may be subject to specific regulations regarding their use and the keeping of electronic records. Customer is responsible for determining whether any particular document is (i) subject to an exception to applicable electronic signature laws; (ii) subject to any particular agency rules; or (iii) can be legally formed using Electronic or Digital Signatures.

Consumer protection or similar laws or regulations may impose specific requirements with respect to electronic transactions involving one or more "consumers," such as requirements that the consumer consent to the method of contracting and/or that the consumer be provided with a copy, or access to a copy, of a paper or other non-electronic, written record of the transaction. Customer is responsible for (i) determining whether any particular transaction involves a "consumer"; (ii) obtaining any required consents or determining if any such consents have been withdrawn; (iii) providing any information or disclosures in connection with any attempt to obtain any

such consents; and (iv) complying with any other special requirements.

6. Fees; Renewal. If Customer purchases a Product Pack for only D-Sign or E-Sign Transactions, Customer may purchase transactions of the other transaction type at the Overage rate shown in the Order Summary.

7. Document Storage and Retention. Customer may retrieve electronic copies of its stored documents at any time while this Service Schedule is in effect. If Customer fails to retrieve its documents prior to the termination of this Service Schedule, Customer may request, no later than thirty (30) days after such expiration or termination, that GlobalSign assist Customer in retrieving any stored documents still remaining in the Service, for an additional charge. After the thirty (30) day period, GlobalSign shall have no obligation to maintain or provide any documents and shall have the right to delete all documents and Customer's account.

Service Schedule for Qualified Signing Service (QSS)

This Service Schedule applies only if Customer 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 purchase a Product Pack, and enroll for a mTLS Certificate for connecting to the Service API.

If Certificates must include your 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 (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.

3. Limitations on Use

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

Customer may not request more than the number of timestamps purchased in a Subscription. Customer shall not request more than five (5) Qualified Timestamps per second. Customer shall be responsible for applying any timestamps into the documents. Customer 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 Customer 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. Customer and Signer should ensure that the PINs are requested judiciously and with appropriate gaps to account for communication delays and avoid abuse of the feature

4. Customer Obligations

4.1 Customer 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 Customer's document management system by either using the Service API or software developer kit (SDK) or configuring the Service for Customer'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.

Customer shall notify GlobalSign in the following case: (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.

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

4.2 If Customer is requesting Signatures for Individuals, Customer must perform Identity Validation of the Individual, the Subject of the Certificate. If Customer will request Certificates for its employees only, Customer will act as a Local Registration Authority (LRA). The terms governing Identity Validation for LRAs are detailed in to this Service Schedule.

For each Certificate for an Individual, Customer shall ensure that the Individual accepts and complies with the terms of the Subscriber Agreement applicable to “Subject”.

4.3 If Customer is applying Electronic Seals to documents, Customer must (a) ensure that for each Individual requesting to apply an Electronic Seal, the Individual is authorized to create the seal on behalf of Customer; (b) only submit requests in the name of an actual department at Customer; (c) not submit requests in the name of an Individual; and (d) not submit requests that are inaccurate or misleading.

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

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

In such case, Customer will immediately cease the use of the Service, and GlobalSign has the right to suspend Customer's use of the Service. Customer will promptly remediate the non-compliance and provide evidence of the remediation for review by GlobalSign. Customer will not resume the use of the Service until GlobalSign has reviewed the remediation and has confirmed to Customer that the use of the Service may be resumed.

6. Audit Rights. GlobalSign has the right to audit Customer'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.

Customer will provide GlobalSign and its auditors, other advisors and regulators with all reasonable cooperation, access and assistance in relation to each audit. Within five (5) days of GlobalSign’s request, Customer will make available the requested information. Customer 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 MSA, 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.

Appendix A to QSS Service Schedule

Additional Terms for Local Registration Authority for Qualified Certificates

GlobalSign delegates to Customer ("Customer" or "RA") the Identity Validation of natural persons affiliated with Customer (employees). These terms govern the obligations, requirements, and responsibilities of Customer for the Local Registration Activities ("Activities") performed by Customer.

1. Obligations. RA must comply with the following obligations:

GlobalSign reserves the right to require changes to RA's Activities 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 RA of requested changes with reasonable notice. RA shall promptly implement any requested changes or immediately cease its Activities if requested by GlobalSign.

RA obligations may not be delegated to other third parties without GlobalSign's prior written consent.

2. Security. RA shall apply information security best practices, including:

Human resources: Ensure that employees support the trustworthiness of the operations.
Operational security: Use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.
Network security: Protect the network and systems from attack.
Privacy of personal information: Take appropriate technical and organizational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

3. Identity Validation. To validate the identity of an Individual, RA must: (a) verify the Individual's identity directly by physical presence of the Individual; (b) obtain evidence of the 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, as far as possible, to distinguish the person from others with the same name; (c) ensure that the Individual's identity information submitted by RA to request Certificate and Signatures is for a current employee who has consented to the request; and (d) create and retain records of the evidence obtained (full name, date and place of birth, copy of a nationally recognized Identity Document) for seven (7) years after any certificate based on these records ceases to be valid, with measures that ensure confidentiality and integrity. If RA, during the retention period, is unable or expects to be unable to retain the evidence obtained, RA shall make arrangements with GlobalSign for the retention of evidence.

Identity Validation must be performed using an Identity Document that: (i) contains a photo of the Individual to be identified; (ii) is resistant to manipulation and sufficiently forgery proof (e.g. using security features); and (iii) is valid at the time of certificate request.

In providing the identity information of an Individual, RA may rely on information within an enterprise directory if (y) identity validation of the Individual has been performed in accordance with the obligations of this Section, and (z) identity information is accurate at the time of the request and refers to a valid Identity Document.

4. Other Obligations. RA shall apply the following practices: (a) submit accurate identity information with each Signature request that matches the Identity Document; (b) remove access of the user upon termination of Individual's employment with the RA; (c) ensure that any Subject requesting a Certificate complies with the Subscriber Agreement for the terms applicable to "Subject" for each Qualified Certificate; (d) provide a process to Subject to request revocation of Subject's certificate and/or destruction of Subject's private key; and (e) notify GlobalSign in writing of any failure of RA to comply with obligations in this Section.

5. Questionnaire. Prior to Customer being accepted as an RA, Customer must complete a questionnaire about its security practices in a form prescribed by GlobalSign. Customer may not perform any Activities until such time as GlobalSign, in its sole discretion, provides written approval of Customer as RA.