IGTF CERTIFICATE SUBSCRIBER AGREEMENT

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE PROCEEDING. BY CHECKING "I AGREE" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO IT. THE PURPOSE OF A DIGITAL CERTIFICATE IS TO BIND AN IDENTITY (TYPICALLY YOURS) TO A PUBLIC-PRIVATE KEY PAIR. BY OBTAINING OR USING A CERTIFICATE ISSUED BY CILOGON OSG CA, YOU AGREE TO THE TERMS HEREIN. IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT CHECK ACCEPT OR SUBMIT YOUR CERTIFICATE ORDER. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, PLEASE E-MAIL GOC@OPENSCIENCEGRID.ORG OR CALL 317-278-9699

This IGTF certificate subscriber agreement ("Agreement") is between CILogon OSG CA ("CA") and you, the individual applying for a Certificate ("You"). This Agreement contains the terms and conditions applicable to the issuance and your use of the IGTF certificate. You and the CA agree as follows:

1. YOUR OBLIGATIONS

1.1. **Key Pairs. You shall securely generate and protect your Private Key in accordance with Schedule 1 and the applicable Guidelines on Private Key Protection. You shall keep all Private Keys confidential and use reasonable measures to protect the Private Key from disclosure. If You suspect misuse or Compromise of a Private Key, You shall promptly (within one working day) notify CA, cease using the Certificate, and request Certificate revocation. You are solely responsible for any failure to protect your Private Keys.**

1.2. **Information. You shall, at all times, provide accurate, complete, and true information to CA. If any information provided to CA changes or becomes misleading or inaccurate, then You shall (i) promptly update the information and (ii) within one working day**

after the information changes, cease using and request the revocation of any Certificate including such information. You shall not install or use a Certificate until after You have reviewed and verified the accuracy of the Certificate data.

1.3. Use. You may not share your Certificate or Private Key with another user, including co-workers. You are responsible for any use of the Certificate and any equipment and software required to use the Certificate. You shall use Certificates in compliance with applicable laws and policies (including the CPS, which is incorporated by reference within the Certificate). You shall promptly notify CA if You become aware of a breach of this Agreement. You are responsible for obtaining and maintaining any additional authorizations or licenses necessary to use the Certificate for a specific or particular purpose.

1.4. Restrictions. You may only use a Host Certificate on the servers accessible at the domain names listed in the issued Certificate. You shall not use your Private Key or Certificate to:

(i) operate nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems, or any other system requiring failsafe operation whose failure could lead to injury, death or environmental damage;

(ii) send, upload, distribute or deliver unsolicited bulk correspondence, malicious code, code that is downloaded without a user's consent, or any files or software that may damage the operation of another's computer;

(iii) make misrepresentations about your Certificate, yourself, or your affiliation with any entity, or breach the confidence of a third party;

(iv) modify, sub license, reverse-engineer, or create a derivative work of any Certificate or Private Key or take any action to attack or attempt to disrupt the

trustworthy operation of any Public Key Infrastructure in which your Key Pair or Certificate participates; or

(v) act in a manner that could reasonably result in a civil or criminal action being taken against You, your sponsor, or CA.

2. CERTIFICATE GENERATION AND PROTECTION

2.1. Verification. An agent of OSG will verify your Certificate application in accordance with the applicable policy document (such as CA's Certification Practices Statement) and industry guidelines. Verification is subject to CA's approval, and CA may refuse to issue a Certificate for any reason. CA is not required to provide a reason for the refusal. CA may deliver an issued Certificate in any manner it sees fit.

2.2. Certificate License. Effective immediately after issuance and continuing until the Certificate either expires or is revoked, CA grants You a revocable, non-exclusive, non-transferable license to use the Certificate, for the benefit of the subject identified therein, and in connection with properly licensed and operating cryptographic software, to (i) create Digital Signatures, (ii) encrypt and decrypt communications, and/or (iii) perform other Public Key or Private Key operations. You are solely responsible for any failure to renew or replace a Certificate prior to its expiration.

2.3. Certificate Revocation and Termination. CA may revoke a Certificate, without notice, for the reasons stated in the CPS, including if CA believes revocation is necessary to protect its reputation or business. You shall promptly cease using the Certificate and corresponding Private Key (except to lawfully decrypt previously encrypted communications) upon: (i) revocation of the Certificate, (ii) termination of this Agreement, or (iii) the date when the allowed usage period for the corresponding Private Key expires.

2.4. Obligation on Revocation or Expiration. Applicant

shall promptly cease using the Certificate and corresponding Private Key upon the earlier of (i) revocation of the Certificate or (ii) the date when the allowed usage period for the corresponding Private Key expires.

3. INTELLECTUAL PROPERTY AND INFORMATION

3.1. Ownership. CA retains sole ownership in (i) any Certificates it issues, (ii) all CA trademarks, copyrights, and other intellectual property rights, (iii) the information collected by CA, and (iv) any derivative works of the Certificates, regardless of who suggested or requested the derivative work.

3.2. Publication of Certificate. You consent to (i) CA's public disclosure of information embedded in an issued Certificate, and (ii) CA's transfer of your personal information to CA's servers, which are located inside the United States.

3.3. Storage and Use of Information. CA shall follow the privacy policy posted on its website when receiving and using information from You. CA may modify the privacy policy in its sole discretion.

4. TERM AND TERMINATION

4.1. Term. This Agreement is effective on acceptance and lasts until the earlier of (i) the expiration date of the corresponding Certificate or (ii) the termination of this Agreement by a party as allowed herein.

4.2. Termination. You may terminate this Agreement for convenience by providing 30 days prior notice to CA. CA may immediately terminate this Agreement if (i) You materially breach this Agreement, (ii) CA cannot satisfactorily verify your information, or (iii) if industry standards or regulations change in a way that affects the validity or security of the Certificates. Upon termination, CA may revoke any Certificates issued under this Agreement.

4.3. Survival. All provisions of this Agreement related to proprietary rights (Section 3.1), disclaimer of warranties and limitations on liability (Section 5), and

the miscellaneous provisions (Section 6) survive the termination of the Agreement and continue in full force and effect.

5. DISCLAIMERS AND LIMITATIONS ON LIABILITY

5.1. Remedy. Your sole remedy for a defect in a Certificate is to have CA use reasonable efforts to correct the defect. CA is not obligated to correct a defect if (i) the Certificate was misused, damaged, or modified, (ii) You did not promptly report the defect to CA, or (iii) You breached a provision of this Agreement.

5.2. Warranty Disclaimers. ALL CA PRODUCTS AND SERVICES, INCLUDING CERTIFICATES, ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, CA DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. CA DOES NOT WARRANT THAT ANY PRODUCTS OR SERVICES WILL MEET YOUR EXPECTATIONS OR THAT ACCESS TO PRODUCTS OR SERVICES WILL BE TIMELY OR ERROR-FREE. CA does not guarantee the availability of any products or services and may modify or discontinue a certificate-related offering at any time.

5.3. Limitation on Liability. EXCEPT AS PROVIDED UNDER SECTION 5.5, YOU WAIVE ALL LIABILITY OF CA AND ITS AFFILIATES, AND EACH OF THEIR OFFICERS, DIRECTORS, PARTNERS, EMPLOYEES, CONTRACTORS, AND AGENTS, RESULTING FROM OR CONNECTED TO THIS AGREEMENT. YOU ALSO WAIVE ALL LIABILITY FOR ANY DIRECT, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RELATED TO THIS AGREEMENT OR A CERTIFICATE, INCLUDING ALL DAMAGES FOR LOST PROFITS, REVENUE, USE, OR DATA. THIS WAIVER

APPLIES EVEN IF CA IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES.

5.4. **Liability for Breach. You are liable for any claims (including damages, costs, and defense expenses) that are brought by third parties against CA, its agents, or assignees that are based by your intentional or grossly negligent breach of this Agreement. This includes claims related to the unauthorized use of your Private Key, unless prior to the unauthorized use You notified CA of the compromise and requested revocation of the Certificate**

5.5. **Applicability. The limitations and waivers in this section 5 apply only to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of any claims, (iii) the extent or nature of the damages, or (iv) whether any other provisions of this Agreement have been breached or proven ineffective.**

5.6. **Force Majeure and Internet Frailties. Neither party is liable for any failure or delay in performing its obligations under this Agreement to the extent that the circumstances causing such failure or delay are beyond a party's reasonably control. You acknowledge that the Certificates are subject to the operation and telecommunication infrastructures of the Internet and the operation of your Internet connection services, all of which are beyond CA's control.**

5.7. **Limitation on Actions. Each party shall commence any claim and action arising from this Agreement within one year from the occurrence of events giving rise to a cause of action. Each party waives its right to any claim that is commenced more than one year from the first date on which the cause of action accrued.**

6. **MISCELLANEOUS**

6.1. Conflict Resolution. All provisions for governing law, jurisdiction, and venue for any arbitration, mediation, or other conflict dispute resolution process shall be as specified in the Sponsor Agreement and such provisions apply equally to this Agreement.

6.2. Independent Contractors. Neither party has the power to bind or obligate the other. Each party is responsible for its own expenses.

6.3. Entire Agreement. This Agreement, along with all documents referred to herein, constitutes the entire agreement between the parties with respect to Subscriber's receipt and use of a requested Certificate, superseding all other agreements that may exist.

6.4. Amendments. CA may amend any of its website and any documents listed thereon, including its CPS and privacy policy, provided that such amendments are adopted and implemented in accordance with the Sponsor Agreement and standard industry practices. Your use of a Certificate after the date an amendment is posted to the website constitutes your acceptance of the amendment.

6.5. Waiver. A party's failure to enforce or delay in enforcing a provision of this Agreement does not waive (i) the party's right to enforce the same provision later or (ii) the party's right to enforce any other provision of the Agreement. A waiver is only effective if in writing and signed by the party against whom the waiver is claimed.

6.6. Notices. You shall send all notices in English to goc@opensciencegrid.org; CA shall send notices to You using the email address provided during the Certificate application process. Notices to CA are effective when received; notices to You are effective when sent.

6.7. Assignment. You may not assign your rights or obligations under this Agreement without the prior

written consent of CA. Any transfer without consent is void and a material breach of this Agreement. CA may assign its rights and obligations without your consent.

6.8. Severability. The invalidity or unenforceability of a provision under this Agreement, as determined by an arbitrator, court, or administrative body of competent jurisdiction, does not affect the validity or enforceability of the remainder of this Agreement. The parties shall substitute any invalid or unenforceable provision with a valid or enforceable provision that achieves the same economic, legal, and commercial objectives as the invalid or unenforceable provision.

6.9. Rights of Third Parties. No third party has any rights or remedies under this Agreement.

6.10. Interpretation. The definitive version of this Agreement is written in English. If this Agreement is translated into another language and there is a conflict between the English version and the translated version, the English language version controls. Section headings are for reference and convenience only and are not part of the interpretation of this Agreement.

7. GLOSSARY OF TERMS

"Certificate" means a digitally signed electronic data file issued by CA to a person, group, or role in order to confirm the identity of that entity as possessing the Private Key that corresponds to the Public Key contained in the certificate.

"CPS" refers to CA's written statements of the policies and procedures used to operate its Public Key infrastructure. CA's CPS documents are available at CILogon OSG CA CP/CPS

"Compromise" means evidence that (i) the hardware device used to store a Private Key is missing, (ii) the Private Key was

publicly disclosed, or (iii) that a third party is using a Private Key without authorization.

"Digital Signature" means an encrypted electronic data file which is attached to or logically associated with other electronic data and which (i) identifies and is uniquely linked to the signatory of the electronic data, (ii) is created using means that the signatory can maintain under its sole control, and (iii) is linked in a way so as to make any subsequent changes that have been made to the electronic data detectable.

"Guidelines on Private Key Protection" refers to the guidelines on private key generation and protection published by the PMA in which the CA participates.

"Key Pair" means two mathematically related cryptographic keys' a Private Key and a Public Key.

"Private Key" means the key that is kept secret by You that is used to create Digital Signatures and/or decrypt electronic records or files that were encrypted with the corresponding Public Key.

"Public Key" means your publically disclosed key that is contained in your Certificate and corresponds to the secret Private Key that You use. The Public Key is used by Relying Parties to verify Digital Signatures created by the Private Key and/or to encrypt messages so that they can only be decrypted by You using the corresponding Private Key.

ACCEPTANCE

BY CHECKING "I AGREE", YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTAND THIS AGREEMENT AND THAT YOU AGREE TO COMPLY WITH ITS TERMS. DO NOT CHECK "I AGREE" AND DO NOT PROCEED IF YOU DO NOT ACCEPT THIS AGREEMENT.

SCHEDULE 1
PRIVATE KEY PROTECTION AND USE

1. Private Key Generation. You shall generate your Key Pair using one of the following methods:

a. Inside a secure hardware token;

b. Using trustworthy cryptographic software on a local computer system where You are the sole user and administrator;

c. On a computer system administered by your sponsor or a third party if:

i. The key material is generated using trustworthy cryptographic software,

ii. Access is limited to designated individuals who are subject to and aware of applicable privacy rules and a professional code of conduct,

iii. The private key and pass phrase are not sent in clear text over a network,

iv. The encrypted private key file is not sent over the network unprotected,

v. The system is located in a secure environment, where access is controlled and limited to only authorized personnel, and

vi. A system does not persistently keep pass phrases or plain text private keys for longer than 24 hours; or

2. **Private Key Storage**. You shall store your Private Key using one of the following methods:

a. Protected by a pass phrase on a hardware token from which the Private Key cannot be extracted;

b. In a persistently encrypted form on a computer system where You are the sole user and administrator; or

c. On a computer system administered by your sponsor or a third party if:

i. The Private Key is stored in a persistently encrypted form and protected by a pass phrase,

ii. Data needed to decrypt or use the private key is present only as a result of your action and only for as long as You are using the system,

iii. Administrative access is limited to designated individuals who are subject to and aware of applicable privacy rules and a professional code of conduct,

iv. The systems are located in a secure environment, where access is controlled and limited to only authorized personnel;

v. The private key and pass phrase are not sent in clear text over a network,

vi. The encrypted private key file is not sent over the network unprotected, and

vii. The system does not persistently keep pass phrases or plain text private keys for longer than 24 hours.

3. **Pass Phrases**. You shall use pass phrases that are at least 12 characters long and follow the industry's current best practices.

4. **Third Parties**. If a third party is involved in the generation of storage of a Private Key, then the third party must have a defined data privacy and security policy.