emSign

SUBSCRIBER AGREEMENT

25-October-2018

Version 1.01

ATTENTION: READ CAREFULLY

THIS EMSIGN SUBSCRIBER AGREEMENT (“SUBSCRIBER AGREEMENT”) IS A LEGAL CONTRACT BETWEEN YOU (“SUBSCRIBER”) AND

EMSIGN CA (REFERRED TO AS “EMSIGN CA” AND REPRESENTED BY EMUDHRA TECHNOLOGIES LTD) AND “ISSUING CA” (REFERRED TO AS “ISSUING CA” AND REPRESENTED BY THE ORGANIZATION THAT EMSIGN MAY HAVE CONTRACTED FOR ISSUANCE OF CERTIFICATE) AND “REGISTRATION AUTHORITY” (REFERRED TO AS “RA”

EMSIGN CA, ISSUING CA AND RA ARE COLLECTIVELY REFERRED TO AS “EMSIGN”.

THE SUBSCRIBER IS THE INDIVIDUAL OR LEGAL ENTITY WHO IS IDENTIFIED IN THE SUBJECT NAME FIELDS OF AN END USER CERTIFICATE, OR WHO IS RESPONSIBLE FOR THE REQUEST, INSTALLATION AND MAINTANANCE OF THE SYSTEMS ON WHICH AN EMSIGN CERTIFICATE IS INSTALLED

THE SUBSCRIBER MUST READ AND ACCEPT THE TERMS AND CONDITIONS SET FORTH IN THIS SUBSCRIBER AGREEMENT BEFORE USING AN EMSIGN DIGITAL CERTIFICATE ISSUED TO YOU

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU ARE NOT AUTHORIZED TO USE OR BE THE CERTIFICATE HOLDER OF AN EMSIGN CERTIFICATE AND YOU MUST TERMINATE YOUR APPLICATION OR REQUEST REVOCATION OF SUCH CERTIFICATE.

THE SUBSCRIBER IS CONSIDERED TO HAVE READ AND ACCEPTED THE LATEST CERTIFICATE PRACTICE/CERTIFICATE POLICY STATEMENTS AVAILABLE AT EMSIGN REPOSITORY – HTTP:// REPOSITORY.EMSIGN.COM

THE SUBSCRIBER AGREES THAT THEY HAVE REVIEWED CAREFULLY THE TERMS AND CONDITIONS OF THIS DOCUMENT. FURTHER THE SUBSCRIBER COVENANTS THAT THEY HAVE UNDERSTOOD THE TERMS AND THEIR INTERPRETATIONS AND VOLUNTARILY AGREES TO ACCEPT EACH AND EVERY PROVISION OF THIS DOCUMENT

THE SUBSCRIBER AGREEMENT IS EFFECTIVE AS OF THE DATE OF APPLICATION FOR THE CERTIFICATE.

Terms and Conditions

The headings in this Agreement are for reference purposes only and will not affect the meaning or construction of the terms of this Agreement.

emSign and the Subscriber, intending to be legally bound, agree as follows.

1. ISSUANCE AND USE OF CERTIFICATES

Upon receipt of a completed application from the subscriber and upon emSign's acceptance, emSign shall perform verification as outlined in the CP/CPS and after completion of such verification, emSign may issue the Subscriber one or more Certificates as applied for by the Subscriber.

The Subscriber agrees to provide full information sought by emSign, with the supporting documentary evidence wherever required, for verifying identity and credentials of the Subscriber. The Subscriber undertakes to provide true and correct information and agrees that emSign and any of its authorised persons shall have a right to independently verify the details provided by the Subscriber. The Subscriber further agrees to promptly notify emSign CA of any change in the information furnished by them while making the application for Digital Certificate.

The Subscriber shall use the emSign Certificate in accordance with the terms and conditions of the CP/CPS available on emSign repository.

2. DEFINITIONS

CP/CPS document shall be referred for definitions.

3. FEES

The Subscriber will pay emSign the fees that is set forth in the then-current published fee for the Certificate(s) on its website or the fees that is the contractually agreed upon price for such Certificate(s). Prices for Certificates available for purchase are subject to change. The fee here is only for the services provided by emSign and is not a royalty or license fee. Non-payment of fees constitutes a material breach of this agreement and emSign reserves the right to revoke Subscriber's Certificate and/or suspend or limit Subscriber's access to his emSign account without notice.

All fees for services are exclusive of any taxes however imposed, e.g. GST, VAT, sales tax or income tax. Customer is solely responsible for calculating and paying all tax obligations resulting from Customer's acceptance of this Agreement, including GST, VAT, sales tax or income tax but excluding all taxes based on emSign's income. Customer may not withhold or offset any amount owed to emSign for any reason. If a TDS or withholding or deduction of tax is required by law, then Customer will pay an additional amount that is equal to the amount withheld or deducted, causing emSign to receive a net amount from Customer that is equal to the amount emSign would receive if a withholding or deduction was not required.

4. ROLE AND OBLIGATIONS OF EMSIGN

emSign's role and obligations under this agreement are as follows.

- Act as the Certification Authority for the emSign Certificate and perform its obligations as specified in this agreement and the CP/CPS
- Represent and warrant that emSign has followed the requirements of the CP/CPS in verifying the accuracy of the information contained in the certificate and in issuing the certificate

emSign is not responsible or liable for the cryptographic methods used in connection with the emSign Certificate

5. REPRESENTATIONS AND WARRANTIES OF THE SUBSCRIBER

Subscriber represents and warrants that:

1. The individual accepting this agreement is duly authorized to accept this agreement on the subscriber's behalf and to bind the subscriber to the terms of this agreement.
2. Subscriber is the entity that it claims to be in the emSign PKI's certificate application.
3. The subscriber has full power, corporate or otherwise, to enter into this agreement and perform its obligations under this agreement. And,
4. This agreement and the performance of the subscriber's obligations under this agreement do not violate any third-party agreement to which the subscriber is a party.

Further, the Subscriber represents and warrants that

- Accuracy of Information – Subscriber will provide accurate, complete and truthful information at all times to emSign, both in the Certificate Request and as otherwise requested by emSign.
- Generation and Protection of Private Key – Where applicable, the Subscriber generates its own Key Pair and shall take all reasonable measures to maintain sole control of, keep confidential, and properly protect and secure at all times the Private Key to be included in the requested Certificate(s) and associated data or device, eg: password or token.
  For Code Signing Certificates, it is recommended that the Subscriber will use one of the following options to generate and protect their Code Signing Certificate private keys:
    - A Trusted Platform Module (TPM) that generates and secures a key pair and that can document the Subscriber's private key protection through a TPM key attestation.
- A hardware crypto module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent.Data Retention – The Subscriber agrees to emSign retaining registration information in accordance with emSign data retention policy
- Acceptance of Certificate – The Subscriber shall not use the Certificate until after he/she has reviewed and verified the contents of the Certificate for accuracy and accepted the certificate.
- Use and Restrictions – Subscriber is responsible at subscriber's expense for all equipment and software required to use the certificate, and also be responsible for subscriber's conduct. Subscriber shall promptly inform emSign, in case of any misuse of the certificate. In case of SSL/TLS Certificates, the subscriber shall install the certificate only on the server accessible at the domain name listed in the Certificate. For all kinds of certificates, applicant shall not
    - modify / sub-license the certificate or the private key.
    - make representations about the certificate, except as allowed by emSign.
    - Sign or certify the document or software or website which may damage the operation of others.
    - Impersonate subscriber's affiliation with any entity.
- The Subscriber confirms and agrees that the use of the Certificate is solely in compliance with all applicable laws and solely in accordance with this Subscriber Agreement and the CP/CPS
- The Subscriber acknowledges and accepts that emSign is entitled to revoke the Certificate immediately if the Subscriber violate the terms of the Subscriber agreement or CP/CPS
- Key Generation and Usage – Where the Subscriber generates their own key pairs. Commonly accepted practices must be used to generate the key pair in a secure manner.
- Sharing of Information – The Subscriber consents to emSign sharing information about the subscriber with other CA's or Industry Groups including CA/Browser forum where the Applicant or Subscriber or its Certificate is identified as a source of suspicious activity, the authority to request the certificate could not verified or the Certificate is revoked for reasons other than subscriber request.

- The Subscriber is aware of and has voluntarily given his consent for the publication of the Digital Certificate on the emSign website and he is aware that all information that forms part of a Digital Certificate are public information and may be available to relying parties and/or the general public. The Subscriber agrees that disclosure of any such information by emSign CA shall not violate any right to confidentiality of the Subscriber.
- Termination – The Subscriber shall cease use of the Private Key associated with the Public Key listed in a Certificate upon expiration or revocation of that Certificate.
- Request for Revocation – The Subscriber shall promptly cease using a Certificate and its associated Private Key, and promptly request that emSign revoke the Certificate in the event that
  - any information in the Certificate is, or become, incorrect or inaccurate
  - there is any actual or suspected misuse or compromise of the Subscriber’s Private Key associated with the Public Key listed in the Certificate.
- Subscriber shall comply with all other obligations, if any, as may be contained in the CP/CPS.

6. REVOCATION

Subscriber Digital Certificates issued by emSign will be revoked when the private key associated with the Digital Certificate is compromised or suspected to be compromised or when any of the information on a Digital Certificate changes or becomes obsolete.

Revocation of a Digital Certificate will be done when any of the following conditions are met,

- When such revocation is requested by the Subscriber
- Any information appearing in the Certificate was or becomes inaccurate or misleading;
- Private Key associated with or used to sign the Certificate is compromised or misused;
- When the original certificate request was not authorized by the Subscriber either prior to issuance or retroactively
- The Applicant has lost its rights to a trademark or the domain name listed in the Certificate;
- The subscriber breached a material obligation under the CP/CPS or Subscriber Agreement
- The Certificate was not issued in accordance with the CP, CPS, or applicable industry standards;
- Issuing CA is compromised
- Issuing CA ceases operations or its right to manage Certificates under applicable industry standards was terminated and Issuing CA does not arrange for another CA to provide revocation support
- A government or regulatory order is received by the Issuing CA to revoke a Certificate
- The technical content or format of the Certificate presents an unacceptable security risk to application software vendors, Relying Parties, or others;
- The Subscriber was added as a denied party or prohibited person to a blacklist
- If the Certificate was used to sign, publish, or distribute malware or other harmful content
- If the binding between the subject and the subject’s Public Key in the Certificate is no longer valid
- For Certificates that have organizational affiliation, the Issuing CA or the RA shall require the Affiliated Organization to inform it if the subscriber affiliation changes. If the Affiliated Organization no longer authorizes the affiliation of a Subscriber, then the Issuing CA shall revoke any Certificates issued to that Subscriber containing the organizational affiliation. If an Affiliated Organization terminates its relationship with the Issuing CA or RA such that it no longer provides affiliation information, the Issuer CA shall revoke all Certificates affiliated with that Affiliated Organization.
- Certificate Holder bankruptcy or liquidation.

- Certificate Holder death.
- Non-payment of fees by the Subscriber.

On revocation of the Digital Certificate, the Subscriber shall no longer be able to use the Certificate again and the Subscriber shall be required to submit a new application in order to obtain a new certificate and the requisite fees shall accordingly apply.

7. DISCLAIMER OF WARRANTIES

- Except as expressly stated in this Agreement emSign (including affiliates or any resellers, co-marketers, subcontractors, distributors, agents, suppliers, employees, or directors) disclaims all warranties, express or implied, by operation of law or otherwise, and all products, services and other items are provided "as is" without warranty of any kind.
- emSign (including affiliates or any resellers, co-marketers, subcontractors, distributors, agents, suppliers, employees, or directors) disclaims any implied warranties of merchantability and fitness for a particular purpose as to emSign products and also disclaims implied warranty of workmanlike quality for services provided by emSign.

8. Subscriber privacy and Use of Third Party Databases

emSign PKI follows the privacy policy and Terms of Service posted on its website when receiving and using information from Subscriber.

For the applicants, emSign PKI may validate personal information supplied during the application process against appropriate third-party databases. By entering into this Agreement, the Subscriber consents to such third-party database checks being made. In performing these checks, personal information provided by the Subscriber may be disclosed to registered credit reference agencies, which may keep a record of that information. Such check is done only for identity confirmation, and as such, a credit check is not performed.

When applying for a Certificate, Subscriber consents to processing, disclosure and transfer of the personal information of the subscriber/applicant, to its affiliates, agents and subcontractors, on a global basis, as necessary to validate and issue the Certificate, including processing, disclosure and transfer to countries that may have data protection laws that are less protective than those in the country where Subscriber is located.

9. LIMITATION OF LIABILITY

The Subscriber agrees that neither emSign nor any of its agents and representatives shall be liable for any loss or consequences caused to the Subscriber on account of any damage to the private key or any unauthorized access and use of private key by a third party.

To the extent Issuing CAs under emSign PKI has issued and managed the certificate in accordance with the CP/CPS, Issuing CAs under emSign PKI shall not have any liability to the Subscriber, Relying Party or any Third Parties for any losses or damages suffered as a result of use or reliance on such a certificate.

Issuing CAs under emSign PKI shall be liable to Subscribers or Relying Parties for direct loss arising from any breach of the CP/CPS or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to the following limits per Subscriber or Relying Party or Third Party per

Certificate, provided the Subscriber, the Relying Party or the Third Party is in full compliance of the CP/CPS.

Limits of Liability per Subscriber or Relying party or Third Party per certificate:

(1) US Dollars One Thousand only (USD 1,000/-)
(2) US Dollars Two Thousand only (USD 2,000/-) for Extended validation certificates.

The limit for aggregate maximum liability for all claims related to a single certificate or service shall be a liability of US Dollars Ten Thousand (USD 10,000/- only) or the amount paid by the subscriber in respect of that certificate or service during the past 12 months, whichever is higher.

The aggregate maximum liability for all claims, regardless of the number and source of claims shall be USD 1 million (USD 1,000,000/-) only.

Issuing CA's liability, under emSign PKI, to any person for damages arising under, out of or related in any way to the CP/CPS, Subscriber Agreement, the applicable contract or any related agreement, whether in contract, warranty, tort or otherwise, shall be limited to actual damages suffered by that person. Issuing CAs under emSign PKI shall not be liable for personal injury, loss of data, indirect, consequential, incidental, special, exemplary, or punitive damages with respect to any person, even if emSign PKI has been advised of the possibility of such damages, regardless of how such damages or liability may arise, whether in tort, negligence, equity, contract, statute, common law, or otherwise.

By participating within the Issuing CAs under emSign PKI, any person that participates within the emSign PKI irrevocably agrees that they shall not apply for or otherwise seek either indirect, exemplary, consequential, special, incidental, or punitive damages and irrevocably confirms to Issuing CAs under emSign PKI their acceptance of the foregoing and the fact that emSign has relied upon the foregoing as a condition and inducement to permit that person to participate within the emSign Public Key Infrastructure.

10. INTELLECTUAL PROPERTY RIGHTS

All rights, title, and interest, including copyright and patent rights, to any certificate, deliverables, ideas, know-how, inventions, software or documentation, developed or delivered by emSign to the Subscriber under this Agreement shall be the property of emSign and the IPR shall stay with emSign.

11. KEY ESCROW

The Subscriber, whose encryption private key is escrowed, hereby authorizes emSign CA or Issuing CA to hold the Private Key under an escrow arrangement on issuance of encryption certificate, which shall, in case, be released or disclosed by Issuing CA of emSign PKI to comply with the direction or order of court, tribunal or law enforcement agencies in accordance with applicable legal requirements.

12. INDEMNIFICATION

The Subscriber shall indemnify, defend and hold emSign and its representatives harmless from all claims, damages, demands, liabilities, costs and expenses that are caused to emSign by reason of false, untrue or incomplete information provided by Subscriber.

The Subscriber shall indemnify, defend and hold emSign their employees/officers/staff/personnel/representatives/agents from all claims, damages, demands, liabilities, costs and expenses, arising from

a) Subscriber’s breach of this Agreement.
b) Subscriber’s failure to protect the authentication mechanisms used to secure the Account or Private Key.
c) An allegation that personal injury or property damage caused by the fault or negligence of the Subscriber.
d) Subscriber’s failure to disclose a material fact related to the use or issuance of the Certificate.
e) Reason or of any claim of infringement of the intellectual property rights of any third parties.
f) Any other claim arising after the issuance of Digital Signature Certificate.

13. NOTICES

Whenever Subscriber desires or is required to give any notice, demand, or request to emSign PKI with respect to this Agreement, each such communication shall be in writing and shall be effective only if it is delivered by a courier service that confirms delivery in writing or mailed, certified or registered mail, postage prepaid, return receipt requested, addressed to emSign PKI at one of our International offices as listed at www.emsign.com, This shall be addressed to Legal Department. It can also be sent over email signed by an emSign Certificate to legal@emsign.com. Such communications shall be effective when they are received.

14. FORCE MAJEURE

Neither party shall be in default of any obligation by reason of any failure to perform or delay in performing due to unforeseen circumstances or due to causes beyond such party’s reasonable control, including but not limited to acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, accidents, strikes, failure to obtain export licenses or shortages of transportation, facilities, fuel, energy, labour or materials. If the force majeure event continues for a period of more than one month, emSign shall have the right to terminate this Agreement or undertake such steps as it may deem appropriate.

15. ASSIGNMENT

The Digital Certificate issued to the Subscriber is personal to the Subscriber and the Subscriber cannot assign or otherwise transfer the Certificate.

The Subscriber shall not assign any of its rights or obligations under this agreement without the prior written consent of emSign. Any assignment without consent is void and constitutes a material breach of this agreement. emSign may assign its rights and obligations without the Subscriber’s consent

16. TERM, TERMINATION AND SURVIVAL

The term of this Document shall be effective from the date the Subscriber submits an application for a certificate and the term shall extend till the period the Digital Certificate remains valid and the Subscriber is using the Digital Certificate issued to him. All payment obligations, if any, shall survive any termination or expiration of this Document.

emSign shall be at liberty to forthwith terminate this Agreement without notice in the event the Subscriber fails to comply with any part of his obligation under this Agreement.

Rights and obligations under this Agreement, which by their nature should survive, shall remain in full force and effect notwithstanding any expiry or termination of this Agreement. The invalidity or un-enforceability of any provisions of this Agreement in any jurisdiction shall not affect the validity, legality or enforceability of the remainder of this Agreement in such jurisdiction or the validity, legality or enforceability of this Agreement, including any such provision, in any other jurisdiction, it being intended that all rights and obligations of the Parties hereunder shall be enforceable to the fullest extent permitted by law.

17. 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.

18. SEVERABILITY

If any provision or part of this Document is found by a court of competent jurisdiction or other competent authority to be invalid or unenforceable, it will be enforced to the maximum extent permissible, and the parties hereto agree to replace the illegal or unenforceable provisions with valid provisions which are as close as possible to the illegal or unenforceable provisions in their respective meaning, purpose, and commercial effect.

The invalidity or un-enforceability of any provisions of this Document in any jurisdiction shall not affect the validity, legality or enforceability of the remainder of this Document in such jurisdiction or the validity, legality or enforceability of this Document, including any such provision, in any other jurisdiction, it being intended that all rights and obligations of the Parties hereunder shall be enforceable to the fullest extent permitted by law.

19. THIRD PARTY RIGHTS

No Third Parties shall have any rights or remedies under this Agreement

20. WAIVER

No waiver of any provisions of this Agreement by either party shall be effective unless made in writing. Any waiver of any term or condition of this Agreement shall not be deemed or construed to be a waiver of such term of condition for the future, or any subsequent breach thereof.

21. ENTIRE AGREEMENT

This Agreement represents the complete agreement concerning the application for issuance of Digital Certificate by emSign and the same may be amended in accordance with the terms laid down in CP/CPS from time to time by emSign only. The amended version of CP/CPS is published in the emSign repository (http://www.emSign.com/repository). If any provision of this Agreement is held to be unenforceable, such provision shall be amended only to the extent necessary to make it enforceable.

This Agreement, including CP/CPS, all Annexures, Exhibits and Schedules (if any) forming part of this Agreement or referred to in this Agreement, shall constitute the entire agreement amongst the parties hereto. It shall supersede all prior or contemporaneous oral or written communications, proposals, conditions, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgement or other communication between the parties relating to its subject matter during the term of this Agreement.

22. GOVERNING LAW AND JURISDICTION.

This agreement is governed by the laws of India except in circumstances where issuing CAs under emSign PKI have explicitly agreed with the subscriber / relying party / any other party to be governed by the laws of any other country. The construction and interpretation of this agreement will be in accordance with laws of India or the laws of the agreed jurisdiction as indicated above. Venue with respect to any disputes will be in Bangalore, India or any venue explicitly agreed in the subscriber / relying party / any other party agreement for the certificate with reference to which the dispute arises.