Agreement on Mutual Recognition of Electronic Signatures and Public Key Infrastructure

Preamble:
The Governments of [Country A] and [Country B] (hereafter referred to as "the Parties"),
Recognizing the importance of electronic commerce and the need to promote the use of electronic signatures and Public Key Infrastructure (PKI) in cross-border transactions,

Acknowledging that electronic signatures have the same legal validity and enforceability as traditional signatures,

Desiring to establish a framework for mutual recognition of electronic signatures and PKI, made in accordance with the laws and regulations of each other's respective countries, in order to facilitate cross-border transactions,

Have agreed as follows:

1. Definitions

(a) "Electronic signature" means data in electronic form which is attached to or logically associated with other electronic data and which is used for the purpose of signing a document, record, or other data.
(b) "Signatory" means a natural or legal person or legal entity who signs a document or record using an electronic signature.
(c) "Trusted third party" means an entity that provides services for creating, managing or verifying electronic signatures and is recognized by the laws or regulations of the respective country, and referred to as Certifying Authorities (CA) or a Trust Service Provider (TSP) in accordance to local laws.
(d) "Public Key Infrastructure (PKI)" means the set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

2. Objectives

The objectives of this agreement are to:

(a) Promote the use of electronic signatures and PKI in cross-border transactions.
(b) Ensure that electronic signatures and PKI are legally valid and secure.
(c) Enhance the efficiency and effectiveness of cross-border trade and commerce.
(d) Establish a framework for mutual recognition of electronic signatures and PKI.

3. Applicable Scope

This mutual recognition arrangement is developed with the intention to establish the acceptance of Digitally Signed documents beyond the home country. It enables promote easier acceptance of documents between the countries, and helps prove the authenticity of the documents which are compliant to National PKI Framework of issuing country.

A digital signature is a type of electronic signature that uses a private key to encrypt a message, and a public key to decrypt it. This ensures that the message has not been tampered with and that it was

actually sent by the person claiming to have sent it. National PKI frameworks make the digital signature more reliable by having Trusted Identity attached to it.

For mutual recognition to be effective, the countries involved must have similar laws and regulations in place for the issuance and use of digital signatures. This typically includes laws on the use of digital certificates, the accreditation of certification authorities, and the legal recognition of digital signatures under the law.

This is intended to result in easier trade and investment facilitation between the countries, facilitate rapid development of electronic transactions between the two places, verifiable electronic documents, ensure secure electronic transactions as well as contribute to paper-free environment. This also intends to provide Cross border trust for securing document exchange, and thus enhance businesses to easily execute contracts, as well as enhance the Import/Export trade.

The scope of the data / documents under this agreement includes, but not limited to:

(a) Data/Documents signed by government agencies and/or the regulated entities including digital identities (like National ID, Driver's license, etc), financial documents (eg: Bank statements, certificates, etc)
(b) Contracts signed between businesses and/or organizations
(c) Data/Documents involved in inter-country trade including Import/Export related documents.

This mutual recognition arrangement is applicable to the electronic signatures made using digital certificates (hereinafter referred to as "certificates"), which are issued by a Trusted Third Party under the National PKI Framework of the country.

4. National PKI Framework

A Public Key Infrastructure (PKI) is used to establish trust between different parties in an electronic transaction, such as a digital signature. A National PKI framework refers to the PKI framework established by a country's government or regulatory body for use within that country.

The National PKI framework is designed to provide a secure and reliable infrastructure for digital transactions and services, and it can be used for a wide range of applications such as digital signature, e-commerce, e-government and secure communication.

The level of maturity, security and interoperability of the PKI Framework can vary between countries. The parties shall ensure that there is an established policy or a set of policies (in the form of law or any other manner) acting as a National PKI Framework in their country which stipulates on recognition or licencing of Trust Service Provider / Certifying Authority, and the operational aspects of it. Such National PKI Framework may also have necessary recognition in other local regulations in order to accept Digital Signatures made via Certificates issued under National PKI Framework.

The parties agree that their National PKI Framework complies to meet below requirements.

(a) Legal framework to recognize digital signatures made under National PKI Framework
(b) Supervision methodology to ensure compliance and conformance to national PKI framework
(c) Trustable Identity verification process of the signatory

(d) Adoption of Technical best practices in terms of standards, algorithms, etc
(e) Identification and representation of Trust under National PKI Framework

5. PKI Compliance

There are several globally accepted PKI (Public Key Infrastructure) compliance standards that are recognized as best practices for implementing and maintaining a secure PKI. These PKI compliance standards provide a framework for the implementation and management of PKI systems that promotes security, integrity, and interoperability. By complying with these standards, organizations and governments can ensure that their PKI systems are secure, trustworthy, and globally recognized.

This agreement considers following 2 acceptable standards under this agreement as they being the most widely recognized in the industry:

(a) WebTrust: WebTrust is a set of standards developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) for auditing and certifying CAs. WebTrust certification is widely recognized as a mark of quality and trustworthiness in the PKI industry.
(b) ETSI TS 102 042: This is a technical standard developed by the European Telecommunications Standards Institute (ETSI) that defines requirements for the implementation and management of PKI systems. It promotes interoperability and trust in PKI systems and is widely recognized in Europe and around the world.

The parties agree that their National PKI Framework complies to any one of the above standards in the operation of the Trusted Third Party in the respective country. The compliance shall be in continuous nature and shall remain active with necessary re-certifications for the entire duration of this agreement.

6. Mutual Recognition of Electronic Signatures and PKI

Electronic signatures and PKI made in accordance with the laws and regulations of each other's respective countries shall be recognized as legally binding and shall have the same legal validity and effect as traditional signatures in the other country, subject to the requirements of their respective laws and regulations.

Each Party shall take appropriate measures to ensure the security and integrity of electronic signatures, including the use of reliable electronic signature creation and verification methods.
Each Party shall provide a legal framework for electronic signatures that is consistent with the principles of non-discrimination, technology neutrality, and functional equivalence.

7. Security Requirements

Electronic signatures and PKI must meet the following security requirements to be recognized under this agreement:

(a) They must be uniquely linked to the signatory.
(b) They must be capable of identifying the signatory.
(c) They must be created using means that the signatory can maintain under their sole control.
(d) They must be linked to the data to which they relate in such a manner that any subsequent change to the data is detectable.

8. Trusted Third Parties

Trusted third parties providing electronic signature and PKI services must meet the following requirements:

(a) They must be recognized by the laws or regulations of their respective country.
(b) They must meet the security requirements set forth in this agreement.
(c) They must maintain accurate and reliable records of all electronic signatures and PKI certificates created or verified by them.
(d) They must provide their services in accordance with applicable laws and regulations.

9. Mutual Recognition of PKI

The Parties recognize the validity and legal effect of digital certificates issued by trusted third parties in accordance with their respective laws and regulations. The Parties shall mutually recognize PKI certificates issued by trusted third parties in each other's respective countries as valid and legally binding.

(a) The Parties agree that any digital certificate issued by a trusted third party in one country shall be accepted as valid by the other Party if it meets the following requirements:
    i. The certificate is issued in accordance with the laws and regulations of the issuing country.
    ii. The certificate identifies the signatory and the certificate holder.
    iii. The certificate is linked to the signatory and the certificate holder in a unique and identifiable manner.
    iv. The certificate is created and maintained in a secure manner.
    v. The certificate is not expired, revoked, or suspended.
(b) Each Party may require that digital certificates issued in the other Party's country be accompanied by certain information or documentation to ensure the authenticity and reliability of the certificate.
(c) The Parties shall cooperate and exchange information on their respective PKI frameworks and trusted third parties to ensure the effective implementation and enforcement of this section.
(d) The Parties agree to encourage the use of interoperable and standardized PKI frameworks to facilitate the exchange and recognition of digital certificates between the two countries.
(e) The Parties may periodically review this section to ensure its effectiveness and relevance in the evolving electronic commerce environment.

10. Cooperation and Exchange of Information

The Parties shall cooperate and exchange information to facilitate the implementation and enforcement of this agreement. They shall provide each other with information about their respective laws and regulations relating to electronic signatures, PKI, and trusted third parties. The Parties shall also exchange information on their respective PKI frameworks and trusted third parties to ensure the effective implementation and enforcement of this agreement.

11. Implementation and Enforcement

The Parties agree to take all necessary measures to implement and enforce this agreement, including the exchange of information and cooperation in investigations and enforcement actions.

(a) Each Party shall designate a competent authority responsible for implementing this Agreement.
(b) The competent authorities shall cooperate with each other to promote the use of electronic signatures in cross-border transactions and to resolve any issues that may arise in the implementation of this Agreement.

12. Dispute Resolution

Any dispute arising from the interpretation or implementation of this Agreement shall be resolved amicably by the Parties through consultations and negotiations.

13. Entry into Force and Termination

This agreement shall enter into force on the date of signature by the authorized representatives of the respective countries. It shall remain in force until terminated by either party upon written notice to the other party.

14. Amendments

This agreement may be amended by mutual consent of the Parties in writing.

Signed on [Date of Signature]

[Authorized Representative of Country A]

[Authorized Representative of Country B]