

Arrangement for Mutual Recognition of Electronic Signature Certificates Issued by Hong Kong and Guangdong

In accordance with Supplement V to the “Mainland and Hong Kong Closer Economic Partnership Arrangement” and “Suggestions on the Framework for the Mutual Recognition of Electronic Signature Certificates issued by Hong Kong and Guangdong”, this mutual recognition arrangement is developed with the intention to promote trade and investment facilitation between Hong Kong and Guangdong, facilitate rapid development of electronic transactions between the two places, ensure secure electronic transactions as well as take forward the existing mutual recognition arrangement between Hong Kong and Guangdong.

1. Applicable scope

This mutual recognition arrangement is applicable to the electronic signature certificates or the recognized digital certificates (hereinafter both electronic signature certificates and recognized digital certificates are referred to as “certificates”), the former of which are issued by third party electronic authentication service providers registered in Guangdong under the Electronic Signature Law of the People’s Republic of China whereas the latter issued by recognized certification authorities (RCAs) established under the Electronic Transactions Ordinance of the Hong Kong Special Administrative Region (“HKSAR”), for cross-boundary electronic transactions between Hong Kong and Guangdong.

2. Mutual recognition approach and publication

Under the mutual recognition arrangement, a cross recognition approach shall be adopted with the publication of trust lists.

The Economic and Information Commission of Guangdong Province (“GDEI”) (under the commission of the Ministry of Industry and Information Technology (“MIIT”)) and the Office of the Government Chief Information Officer (“OGCIO”) of HKSAR shall publish their local trust list as well as the other party’s trust list.

3. Application for participating in the mutual recognition scheme

The electronic authentication service providers in Guangdong shall submit their application for participating in the mutual recognition scheme to GDEI, whereas RCAs in Hong

Kong shall submit their application to OGCIO.

The following documents are required for the application:

- (1) An application form for mutual recognition of certificates;
- (2) A Certification Practice Statement (“CPS”) that complies with the “Certificate Policy for Mutual Recognition of Electronic Signature Certificates Issued by Hong Kong and Guangdong” (“Mutual Recognition Certificate Policy”);
- (3) An assessment report issued by an independent third party on the compliance of the CPS with the Mutual Recognition Certificate Policy;
- (4) An assessment report issued by an independent third party on the implementation of the CPS.

4. Approval for participating in the mutual recognition scheme

For the applications from local electronic authentication service providers, GDEI shall perform preliminary examination before submitting them to MIIT for approval. OGCIO shall approve applications from local RCAs.

GDEI or OGCIO shall notify the other party of the approval results. GDEI or OGCIO shall publish their trust list after performing their respective legal procedures.

5. Suspension and termination of mutual recognition

Under the following circumstances, GDEI or OGCIO shall suspend or terminate the mutual recognition of certificates:

- (1) GDEI or OGCIO has received a suspension or termination request from their local participating electronic authentication service provider;
- (2) A participating electronic authentication service provider has violated the requirement(s) of this mutual recognition arrangement and refused to make corrective action(s), or if violation or non-compliance is found in the certificate issuance process.

GDEI or OGCIO shall timely inform the other party of the suspension or termination of mutual recognition of certificates in writing. GDEI or OGCIO shall remove the corresponding certificate type(s) as well as the electronic authentication service provider concerned from the trust list, and then inform the other party and the electronic authentication service provider concerned of this in writing. GDEI shall timely report this to the Department of Information Security Coordination of MIIT for record.

6. Duties and obligations of electronic authentication service providers

The participating electronic authentication service providers shall perform the following duties and obligations:

- (1) Be qualified in annual inspection/assessment, and be subject to special assessment as required;
- (2) Their CPS complies with the Mutual Recognition Certificate Policy, and an independent third party shall be commissioned to conduct assessment as required;
- (3) Their certificate services are operated in line with their CPS, and an independent third party shall be commissioned to conduct assessment;
- (4) The electronic authentication service providers in Guangdong shall establish sound security management and internal audit systems, whereas RCAs in Hong Kong shall enhance their security management and monitoring functions;
- (5) They establish a sound information protection system for the protection of information relevant to electronic authentication;
- (6) Certificates issued for mutual recognition contain the following content accurately:
 1. Name of issuing certification authority;
 2. Name of certificate holder;
 3. Certificate serial number;
 4. Expiry date of certificate;
 5. Data for validating certificate holder's signature;
 6. Signature of issuing certification authority;

7. Certificate policy object identifier;
8. Other required contents.

(7) The key pairs generated for issuing certificates and certificate status information shall comply with the requirements of the Mutual Recognition Certificate Policy. The hardware devices for generating a key pair shall comply with local regulatory requirements.

The electronic authentication service providers in Guangdong shall timely report the new certificates issued by them to GDEI for record. GDEI shall timely report the new certificates issued by electronic authentication service providers to the Department of Information Security Coordination of MIIT for record. RCAs in Hong Kong shall timely report the new certificates issued by them to OGCIO for record.

7. Management of mutual recognition of certificates

(1) The Guangdong-Hong Kong Working Group on Pilot Applications of Mutual Recognition of Electronic Signature Certificates (the “Working Group”), established by Department of Information Security Coordination of MIIT, Department of International Cooperation of MIIT, GDEI and OGCIO, is responsible for the formulation, publication, updating and interpretation of the Mutual Recognition Certificate Policy as well as working out the relevant details of this mutual recognition arrangement.

(2) The Working Group will assign certificate policy object identifiers to certificates that comply with the Mutual Recognition Certificate Policy;

(3) The Mainland and Hong Kong shall supervise their local participating electronic authentication service providers in accordance with their respective laws and regulations to ensure that they can effectively perform their duties and obligations.

(4) The eligibility of the “independent third party” mentioned in this mutual recognition arrangement shall be determined by the local regulatory authorities in accordance with the local laws and regulations.

8. Publication and effective date

This mutual recognition arrangement shall become effective upon its publication date.