DNSSEC Practice Statement
for
.HK and .香港 top level domain names

V1.2

Contents

1. INTRODUCTION

This document is a statement of security practices of HKIRC that are applied in the DNSSEC operations for the .HK and .香港 top level domain names.

This document conforms with the RFC 6841 DNSSEC Policy & Practice Statement Framework (http://www.ietf.org/rfc/rfc6841.txt).

1.1. Overview

DNSSEC (DNS Security Extensions) is a set of specifications that enable the authentication of DNS data and also make it possible to ensure that content has not been modified during transfer.

DNSSEC are described in the follow RFCs.

RFC 4033	DNS Security Introduction and Requirements
RFC 4034	Resource Records for the DNS Security Extensions
RFC 4035	Protocol Modifications for the DNS Security Extensions
RFC 4509	Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)
RFC 5155	DNS Security (DNSSEC) Hashed Authenticated Denial of Existence

RFC 5933	Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSE
RFC 6605	Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC
RFC 6781	DNSSEC Operational Practices, Version 2
RFC 6944	Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status
RFC 2536	DSA KEYs and SIGs in the Domain Name System (DNS)
RFC 2539	Storage of Diffie-Hellman Keys in the Domain Name System (DNS)
RFC 3110	RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)
RFC 3226	DNSSEC and IPv6 A6 aware server/resolver message size requirements
RFC 4033	DNS Security Introduction and Requirements
RFC 4034	Resource Records for the DNS Security Extensions
RFC 4035	Protocol Modifications for the DNS Security Extensions
RFC 4398	Storing Certificates in the Domain Name System (DNS)
RFC 4509	Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)
RFC 5155	DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
RFC 5702	Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC
RFC 5933	Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSE

RFC 6605	Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC
RFC 6781	DNSSEC Operational Practices, Version 2
RFC 6944	Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status

1.2. Document name and identification

Document title: DNSSEC Practice Statement for the .HK and .香港 top level domain names (HK DPS)

Version: 1.2

Created on: 6 July 2017

Effective on: 10 July 2017

1.2.1. Community and applicability

The associated entities and their roles are described in this section.

1.2.2. Registry

HKIRC is the Registry for the .HK and .香港 domain names.

The Registry administrates the registrations of .HK and .香港 domain names and operates DNS servers for the .HK and .香港 zones.

The Registry is responsible for generating key pairs and protecting the confidentiality of the private component of the Key Signing Keys and Zone Signing Keys.

The Registry is also responsible for securely signing all authoritative DNS resource records in the .HK and .香港 zone.

The Registry is responsible for the registration and maintenance of DS resource records in the root zone.

1.2.3. Registrar

A Registrar is the party that is responsible for the administration and management of domain names of behalf of the Registrant. The Registrar handles the registration, maintenance and management of a Registrants domain name and is an accredited Registry's partner.

The Registrar is responsible for securely identifying the Registrant of a domain. The Registrar is responsible for adding, removing or updating specified DS records for each domain at the request of the Registrant.

The relation between the Registry and a Registrar is regulated in the Registry-Registrar Agreement which may be found as a whole in the HKIRC websites.

1.2.4. Registrant

A Registrant is an entity who has registered .HK and .香港 domain name(s). Registrants are responsible for generating and protecting their own keys, and registering and maintaining the DS records through the Registrar.

To enables the authentication and data integrity verification for the registered domain names, the Registrant composes the digital signatures on Registrant's zone using their own keys.

The Registrant is responsible for issuing an emergency key rollover if keys are suspected of being compromised or have been lost.

1.2.5. Relying Party

The relying party is the entity relying on DNSSEC such as validating resolvers and other applications. The relying party is responsible for configuring and updating the appropriate DNSSEC trust anchors.

1.2.6. Auditor

Auditor is an entity who audits whether the Registry's DNSSEC Service is operated along with .HK and .香港 DPS or not.

1.2.7. Applicability

Each Registrant is responsible for determining the relevant level of security for their domain. This DPS is exclusively applicable to the .HK and .香港 top-level domain names.

With the support of this DPS, the relying party can determine the level of trust they may assign to DNSSEC in the .HK and .香港 domain and assess their own risk.

The Registrant Zones are under Registrant's policy and outside the scope of HK DPS.

1.3. Specification administration

1.3.1. Specification administration organization

Hong Kong Internet Registration Corporation Limited (HKIRC)

1.3.2. Contact Information

Hong Kong Internet Registration Corporation Limited

Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong

Telephone: (852) 2319 1313

Fax: (852) 2319 2626

Email: info@hkirc.hk

https://www.hkirc.hk

1.3.3. Specification change procedures

Amendments to this DPS are either made in the form of amendments to the existing document or the publication of a new version of the document. This DPS and amendments to it are published at HKIRC websites.

Only the most recent version of this DPS is applicable.

HKIRC reserves the right to amend the DPS without notification for amendments that are not designated as significant. It is in the sole discretion of HKIRC to designate changes as significant, in which case HKIRC will provide notice. Any changes will be approved by HKIRC and may be effective immediately upon publication.

2. PUBLICATION AND REPOSITORIES

2.1. Repositories

2.1.1. Operational entity

The entity that operates repositories is HKIRC as a Registry.

2.1.2. Locations of the repositories

HKIRC publishes DNSSEC-relevant information on the website at https://www.hkirc.hk

2.1.3. Access controls on repositories

Information published at the HKIRC website is available to the general public for read only access and is protected against unauthorized adding, deletion or modification of the content on the website.

2.2. Publication of public keys

The DS record of the .HK and .香港 zones are registered into and published in the root zone. The Registry does not explicitly publish KSK public key of the HK zone as a trust anchor.

3. OPERATIONAL REQUIREMENTS

3.1. Meaning of domain names

Domain names are defined in the “Domain Name Registration Policies, Procedures and Guidelines” published in HKIRC websites.

3.2. Identification and authentication of child zone manager

The identification and authentication of the Registrant is conducted by the Registrar. Registrar is responsible to comply with the Registrar agreement contracted between the Registry and the Registrar.

3.3. Registration of delegation signer (DS) resource records

DNSSEC is activated by at least one DS record for the zone being sent from the Registrar to the Registry and thus being published in the DNS, which established a chain of trust to the child zone. The Registry presumes that the DS record is correct and will not perform any specific controls.

The Registry accepts DS records through the system interface from each Registrar. The DS record must be valid and sent in the suitable format. More than one DS records (up to a maximum limit of 5) can be registered per domain name.

3.3.1. Who can request registration

The Registry accepts DS records registration from authenticated Registrars. Registrar should confirm the intentions of the registration with the Registrant before requesting the registration to the Registry.

3.3.2. Procedure for registration request

The Registry accepts authenticated registrars to add DS record through the EPP System interface according to RFC 5910 (Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)) and manually via web panel. Any valid DS record will be accepted by the registry, and no checks are performed as to the accuracy of the trust anchor with respect to the child zone's KSK.

3.3.3. Emergency registration request

There is no provision for emergency registration request. All registration requests must be executed through authenticated registrars. Please refer to 3.3.2 for Procedure for registration request.

3.4. Method to prove possession of private key

The Registry does not conduct any controls with the aims of validating the Registrant as the manager of a private key. The Registrar is responsible for conducting the controls that are required and those deemed necessary.

3.5. Removal of resource DS records

A DS record is deregistered by sending a request from the Registrar to the Registry. The deregistration of all DS records will deactivate the DNSSEC security mechanism for the zone in question.

3.5.1. Who can request removal

The Registry removes DS records for a Registrant based on the request from Registrar. Registrar should confirm the intentions of the registration with the Registrant before requesting the removal.

3.5.2. Procedure for removal request

The Registry accepts authenticated registrars to remove DS record through the EPP System interface according to RFC 5910 (Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)) and manually via web panel. The removal of all DS records for a domain name will remove the chain of trust between the top-level domain zone and the child zone.

3.5.3. Emergency removal request

There is no provision for emergency removal request. All DS record removals must be executed through authenticated registrars. Please refer to 3.5.2 for Procedure for removal request.

4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

4.1. Physical controls

4.1.1. Site location and construction

The Registry installs and operate important equipment related to .HK and .香港 top level domain names in two fully operational and geographically dispersed locations in Hong Kong. All equipment are protected within a physical perimeter with access control. Both sites have equipped with facility protection in terms of physical security, power supply, air conditioning, fire and water protection.

4.1.2. Physical access

Physical access to the protected environment is limited to authorized personnel. Entry is logged and the environment is continuously monitored.

All equipment is located in locked cabinets, with limited access to authorized personnel only.

All access to facilities is logged as well as 24x7 CCTV monitoring. All log and recording are kept for at least one year.

Physical access procedure:

1. When visitors arrive at the security front desk, they are required to provide identification for registration.

2. Guards contact NOC staff to verify visitors' access permissions.

3. Access card will be provided and visitors are allowed to access to the data hall.

4. NOC staff escort visitors to the rack facility and unlock racks.

5. Before leaving, visitors must sign-out at security front desk.

4.1.3. Power and air conditioning

Power is provided to the sites through separate sources. In the event of power outages, power is provided by UPS until the backup power systems came into operation.

4.1.4. Water exposures

The sites has water protection and detection system.

4.1.5. Fire prevention and protection

The sites are equipped with fire detection and extinguishing systems.

4.1.6. Media storage

All software, data-containing media, auditing information, archives and the corresponding backup information are stored in secure local or remote device for

appropriate physical and logical access to prevent them from accidental damage or from being exposed to unauthorized personnel.

4.1.7. Waste disposal

Disposed storage media and other material that may contain sensitive information are destroyed in a secure manner, either by the Registry or a contracted party.

4.1.8. Off-site backup

The Registry performs regular backups of critical data, audit logging data and other sensitive information. An off-site facility is leveraged for storage of backup media. Physical access to the off-site facility is limited to authorized personnel. The off-site facility is geographically separated from where the backup is performed.

4.2. Procedural controls

4.2.1. Trusted roles

Trusted roles are held by persons that are able to affect the zone file's content, the management of private keys. The trusted roles exist for providing DNSSEC services for the .hk and .香港 zone in and M of N approach. Where a minimum of M trusted personnel is required to complete a trusted role and where M is never equal to 1. The Trusted roles are:

1. Systems Administrator, SA – Prime & Backup
2. Security Officer, SO – Prime & Backup
3. Internal Witness, IW – Prime & Backup

4.2.2. Number of persons required per task

Pre-key Roll Ceremony	3	SA, SO, IW
Post-key Roll Ceremony	3	SA, SO, IW
Initialization or restoration of signing appliances	2	SA, SO
Configuration of signing appliances	2	SA, SO

None of these operations may be performed in the presence of unauthorized people.

The Registry ensure the segregation of duties based on roles and to ensure that at least two person in Trusted Role to perform sensitive tasks.

4.2.3. Identification and authentication for each role

Only the Registry staff members who have signed a HKIRC employment agreement may hold a trusted role's role. Valid identification must be provided before credentials for system access are provided.

4.2.4. Tasks requiring separation of duties

Sensitive tasks require separation of duties include have access to or control cryptographic operations that affect:

- Generation, activation, protection of private key of Zone Signing Key (ZSK) and Key Signing Key (KSK);
- Use of private keys to generation and signing of zone data;
- Export and import of any components; And
- Publication of chain-of-trust between root zone and .hk and .香港.

4.3. Personnel controls

4.3.1. Qualifications, experience, and clearance requirements

Persons who have "Trusted Role" as described in 4.2.1 are limited to full time employees of the Registry or those who are specifically approved by the Registry.

4.3.2. Background check procedures

For the trusted roles in Section 4.2.1, the following background checks are included:

- Candidate resume
- Previous employments
- Reference check

Using this information, the registry would then decide on a case by case basis if the individual considered for a trusted role is suitable or not.

4.3.3. Training requirements

The Registry gives training to personnel in charge of the DNSSEC Service. Before the person is taking up the role, the required trainings for the roles are provided. When there is changes to the operation, trainings associated with the changes are provided.

4.3.4. Job rotation frequency and sequence

The responsibility for conducting operations is rotated on each occasion between the people who hold a trusted role.

4.3.5. Sanctions for unauthorized actions

Sanctions resulting from unauthorized actions are regulated by the HR function at HKIRC.

4.3.6. Contracting personnel requirements

In certain circumstances, the Registry may need to use contractors as a supplement to full-time employees. Contractors are subject to the same responsibility agreements and background checks as trusted roles. All contractors' staff is allowed to access to the system only with approval by the registry and their work must be under guidance and supervision by the Registry trusted roles.

4.3.7. Documentation supplied to personnel

The Registry and IT operations supply the documentation necessary for the individual employee to perform their work task in a secure and satisfactory manner.

4.4. Audit logging procedures

4.4.1. Types of events recorded

The Registry maintains logging to a centralized logging server for analysis. The Registry will log a minimum of:

- Key generation/destruction/export/import
- Signing system access/backup/restoration
- Successful/Unsuccessful zone signing events
- Hardware failures
- Successful and unsuccessful system access

4.4.2. Frequency of processing log

Logs are continuously monitored through automated control and sufficiently frequently through manual controls to detect any anomalies.

4.4.3. Retention period for audit log information

Log information is stored in systems for not less than 12 months.

4.4.4. Protection of audit log

All electronic log information is stored at the protected operations facilities. The logging system is protected against unauthorized viewing and the manipulation of information.

4.4.5. Audit log backup procedures

All electronic log information is securely backed up on a monthly basis and is stored separately from the system in a secure location.

4.4.6. Audit collection system

Automated audit data is generated and recorded at the application, network, and operating system level. Manually generated audit data is recorded by the Registry personnel and stored using methods for physical and fire protection mentioned in Section 4.1.

4.4.7. Vulnerability assessments

Vulnerability assessments are conducted against all data center sites on a regular basis. Any issues identified result in a risk management issue and are resolved using project management techniques to resolve and track.

4.5. Compromise and disaster recovery

4.5.1. Incident and compromise handling procedures

All incidents are handled in accordance with the Registry's incident handling procedures. The incident handling procedure includes investigating the cause of the incident, what effects the incident has had or may have had, measures to prevent the incident from recurring and forms to further report this information.

An incident that involves suspicion that a private key has been compromised leads to the immediate rollover of keys pursuant to the procedures indicated in chapter 4.5.3.

4.5.2. Corrupted computing resources, software, and/or data

In the event of corruption, the incident management procedures shall be initiated and appropriate measures shall be taken.

4.5.3. Entity private key compromise procedures

Suspicion that a private key has been compromised or misused leads to a controlled key rollover as follows:

- If a zone signing key is suspected of having been compromised, it will immediately be removed from production and stopped being used. If necessary, a new ZSK will be generated and the old key will be removed from

the key set as soon as its signatures have expired or timed out.

- If a KSK is suspected of having been compromised, a new key will be generated and put into immediate use, in parallel with the old key. The old KSK will remain in place and be used to sign key sets until such time as it can be considered sufficiently safe to remove the key taking into account the risk for system disruptions in relation to the risk that the compromised key presents. Affected registrars will be notified by email about the information of the emergency KSK roll.

4.5.4. Business Continuity and IT Disaster Recovery Capabilities

The Registry has a IT disaster recovery plan that ensures that operation-critical production can be switched over between the two operation facilities. The facilities are equivalent in terms of physical and logistical protection. Information is replicated between the facilities.

4.6. Entity termination

If the Registry must discontinue DNSSEC for any reason and return to an unsigned position, this will take place in an orderly manner. If operations are to be transferred to another party, the Registry will participate in the transition so as to make it as smooth as possible.

5. TECHNICAL SECURITY CONTROLS

5.1. Key pair generation and installation

5.1.1. Key pair generation

All key pairs are generated on the signing systems according to parameters set by the Registry operational team. The signing systems' cryptographic modules meet the requirements of FIPS 140-2 level 2. The public key is automatically inserted in the TLD zone file as a DNSKEY resource record as part of the signing process. A DS record is made available for submission to the parent (root) zone. Key Roll Ceremony process will be witness and subject to the Registry internal audit.

The signing system maintains the separation of the KSK from the ZSK and manages the use of each key pair as appropriate. Each key is used for only one zone.

5.1.2. Public key delivery

The public key is automatically inserted in the TLD zone file as a DNSKEY resource record as part of the signing process. A DS record is made available for submission to the parent (root) zone.

5.1.3. Public key parameters generation and quality checking

Key parameters, including key event dates (activation, deactivation, etc), length and algorithm type, are verified by the SA, SO and the IW. These include:

a. Key Signing Key
b. Zone Signing Key

5.1.4. Key usage purposes

The Registry uses the signing keys only for generating signatures for the .HK and .香港 zones and does not use them for any other purposes.

5.2. Private key protection and cryptographic module engineering controls

5.2.1. Cryptographic module standards and controls

All signing systems are FIPS 140-2 level 2 certified. No unencrypted access to the private key is permitted.

5.2.2. Private key (m-of-n) multi-person control

The Registry has implemented technical and procedural mechanisms that require the participation of multiple trusted roles to perform sensitive cryptographic operations.

Access to the signing system is restricted to personnel in trusted roles as identified in Section 4.2.1. Number of trusted personnel required for task is described in Section 4.2.2. And tasks require separation of duties are described in Section 4.2.4. The access to the signing system has a threshold number of trusted roles of 2.

5.2.3. Private key escrow

The Registry does not apply a key escrow.

5.2.4. Private key backup

The private key are automatically backed up in encrypted form and stored in the protected facilities. For facilities and access control information, refer to Section 4.1.1 and 4.1.2.

All facilities are protected by:

1. Gas based fire suppression system with pre-action dry pipe water fire suppression system
2. Fire detection system (E.g. smoke and/or heat detector)
3. Water leakage detection system to detect possible water damage due to leakage or flooding
4. 24x7 cooling and humidity control with redundancy in case of break down

5.2.5. Private key storage on cryptographic module

Private keys are stored within the cryptographic module in an encrypted format.

5.2.6. Private key archival

Private keys that are no longer used are not archived in any other form than as backup copies.

5.2.7. Private key transfer into or from a cryptographic module

All Private key leave the cryptographic module in encrypted form. Key is only transferred between trusted signing system through SSH tunnel within a trusted network in the Registry data centers.

5.2.8. Method of activating private key

Private keys are activated by configuring an activation and publication date when generating the relevant key pair. These date are verified during the quality checking detailed in Section 5.1.3.

5.2.9. Method of deactivating private key

Private keys are deactivated automatically after a new private key is activated as in 5.2.8.

5.2.10. Method of destroying private key

No efforts are made to destroy private keys after their operational period has expired as they have become invalid. After their usage period they are removed from the signing system to avoid accidental reuse.

5.3. Other aspects of key pair management

5.3.1. Public key archival

Public keys that are no longer used are not archived in any other form than as backup copies.

5.3.2. Life cycle states for management

The following is the life cycle states of KSK for key management:

- Generation of KSK
- Registration of KSK into the HK zone and the root zone
- Deletion of KSK from the root zone and the HK zone
- Removal of KSK

The following is the life cycle states of ZSK for key management:

- Generation of ZSK
- Registration of ZSK into the HK zone
- Activation of ZSK
- Inactivation of ZSK
- Deletion of ZSK from the HK zone
- Removal of ZSK

5.3.3. Key usage periods

Keys become invalid as they are taken out of production according to period set out in Section 6.4. Old keys are not reused.

5.4. Activation data

5.4.1. Activation data generation and installation

Each personnel with trusted roles are responsible to create their own activation data (credentials) of at least 12 characters of varying nature.

5.4.2. Activation data protection

Each personnel is acknowledged and agreed they are responsible for protecting their activation data (credentials) in a secure fashion. On the suspicion of compromised activation data (credentials), the personnel must immediately change it.

5.4.3. Other aspects of activation data

In the event of an emergency, there is a sealed and tamper evident envelope in a secure location that contains activation data.

5.5. Computer Security Controls

All critical components of the Registry's systems are placed in the protected facilities in accordance with 4.1. Access to the server's operating systems is limited to individuals that require this for their work, meaning system administrators. All access is logged and is traceable at the individual level.

5.6. Network Security Controls

The Registry has sectioned networks that are divided into various security zones with secured communications in-between. The Registry uses firewall to protect the production network from both internal and external intrusion and to limit the nature and source of network activities that may access production systems that are related to key signing activities. Logging is conducted in the firewalls. Transmission of classified information is protected with suitable method (e.g. encryption).

All firewall components generate logs which are collected, analyzed and retained.

5.7. Timestamping

The Registry retrieves time from a reliable time source (e.g. the time services provided by The Hong Kong Observatory). Time stamps are used for log information and validity time for signatures.

5.8. Life Cycle Technical Controls

5.8.1. System development controls

The Registry controls the processes of system developments. The development model includes specifying the functional and security requirements, as well as systematic testing and regression tests.

5.8.2. Security management controls

The Registry has technologies and policies in place to control and monitor the configuration of its systems, this includes monitoring of access on all systems, configuration changes and package install or updates. The Registry regularly conduct risk assessment and implement preventive measures, detective measures and corrective actions. The Registry also conducts regular security audits of the system.

5.8.3. Life cycle security controls

The signing system is designed to require a minimum of maintenance. Updates critical to the security and operations of the signing system will be applied after formal testing and approval. The origin of all software and firmware will be securely authenticated by available means. Critical hardware components of the signing system will be procured directly from the manufacturer and transported to their destination in the secure facility. All hardware will be decommissioned well before the specified lifetime expectancy.

The Registry regularly conduct risk assessment and implement preventive measures, detective measures and corrective actions. The Registry also conducts regular security audits of the system.

6. ZONE SIGNING

6.1. Key lengths, key types, and algorithms

Key length of KSK is 2048 bits.

Key length of ZSK is 1024 bits.

The algorithm for both KSK and ZSK is RSASHA256.

6.2. Authenticated denial of existence

For authenticated denial of existence, NSEC3 records with Opt-Out flag specified in RFC 5155 is adopted.

6.3. Signature format

The signature format is RSA/SHA-256 specified in RFC 5702.

6.4. Key rollover

6.4.1. Zone signing key roll-over

ZSK rollover is carried out on a monthly basis by the pre-publish method.

6.4.2. Key signing key roll-over

KSK rollover is carried out on an annual basis by the double signature.

6.5. Signature lifetime and re-signing frequency

Signatures are valid for 30 days.

Signatures are regenerated every day.

6.6. Verification of resource records

The Registry verifies that all resource records are valid in accordance with the current protocol standards prior to distribution.

6.7. Resource records time-to-live

DNSKEY = 1 day

DS = 1 day

NSEC3 = 1 day

RRSIG = varies depending on the RR covered

7. COMPLIANCE AUDIT

7.1. Frequency of entity compliance audit

The Registry conducts security audit regularly. Current frequency is once every 2 years.

7.2. Identity/qualifications of auditor

The auditor shall be able to demonstrate proficiency in IT security, DNS and DNSSEC.

7.3. Auditor's relationship to audited party

An external auditing manager shall be appointed for the audit.

7.4. Topics covered by audit

The Registry's DPS is covered by the audit.

7.5. Actions taken as a result of deficiency

The result will be followed up aiming to correct any discrepancy with the HK DPS.

7.6. Communication of results

A written report will be submitted to the Registry for the record and to follow up.

8. LEGAL MATTERS

The Registry has no legal responsibility for the matters described in HK DPS.

8.1. Limitations of liability

The limitations of liability between the Registry and the Registrar are regulated by the relevant section of the Registrar Agreement.

The limitations of liability toward the Registrant are regulated by the relevant section of the Domain Name Registration Policies, Procedures and Guidelines for .hk and .香港 domain names

8.2. Governing law and jurisdiction

The HK DPS shall be governed by and interpreted in accordance with the laws of the Hong Kong Special Administrative Region of the People's Republic of China (HKSAR). The parties hereby submit to the exclusive jurisdiction of the courts of the HKSAR.