Hong Kong Internet
Registration Corporation Limited
香港互聯網註冊管理有限公司

Domain Name System Security Extensions (DNSSEC) Implementation Project

Request for Proposal

Version 1.2
Date: 6 April 2016

Hong Kong Internet Registration Corporation Limited

Unit 2002-2005, 20/F FWD Financial Centre, 308 Des Voeux Road Central, Sheung Wan, Hong Kong.
Tel.: +852 2319 1313 Fax: +852 2319 2626
Email: enquiry@hkirc.hk Website: www.hkirc.hk

IMPORTANT NOTICE

Table of Contents

1. Summary

HKIRC is going to commission an external Service Provider to implement DNSSEC for the .hk and .香港 and their sub-domains. The service shall provide complete design, building and integration of DNSSEC solution to HKDNR's existing system. The Service Provider shall provide all software, hardware and professional services in order to implement their DNSSEC solution in HKDNR environment.

HKIRC is looking for a service provider(s) ("the Contractor") to provide and setup for the above services.

The scope of service is detailed in section 4 and 5 of this document.

Parties interested in providing this service shall submit **Expression of Interest (EOI) by 21st, March 2015**. For those who have submitted EOI, they should **submit proposal** (see Appendix D) to the Group **no later than 5:30pm on 27th April 2015**.

The Contractor should submit Expression of Interest by email to HKIRC contacts (refer to Appendix D - HKIRC Proposal Requirements, electronic copy). The Contractor must provide their information as required in the proposal cover page (Appendix D, 1.3 Cover Page).

2. Definitions

The following terms are defined as in this section unless otherwise specified.

“The Contractor” means the company who will provide the Services after award of contract.

“HKIRC” means Hong Kong Internet Registration Corporation Limited.

“HKDNR” means Hong Kong Domain Name Registration Company Limited, a wholly-owned subsidiary of HKIRC, the company requesting the proposal for “the Services”.

“ISMS” means Information Security Management System. It consists of an information security organization and a set of policies, guidelines and procedures concerned with information security management.

“The Services” means the DNSSEC Implementation Service with requirements stipulated in Section 4 of this document.

“RFP” means this Request for Proposal

“Tenderer” means the company who will submit proposal to provide the Services

3. About HKIRC

Hong Kong Internet Registration Corporation Limited (HKIRC) is a non-profit-distributing and non-statutory corporation responsible for the administration of Internet domain names under '.hk' and '.香港' country-code top level domains. HKIRC provides registration services through its registrars and its wholly-owned subsidiary, Hong Kong Domain Name Registration Company Limited (HKDNR), for domain names ending with '.com.hk', '.org.hk', '.gov.hk', '.edu.hk', '.net.hk', '.idv.hk', '.公司.香港', '.組織.香港', '.政府.香港', '.教育.香港', '.網絡.香港', '.個人.香港'. '.hk' and '.香港'.

HKIRC endeavours to be:

- Cost-conscious but not profit-orientated
- Customer-orientated
- Non-discriminatory
- Efficient and effective
- Proactive and forward-looking

More information about HKIRC can be found at http://www.hkirc.hk .

HKIRC and HKDNR are listed as public bodies under the Prevention of Bribery Ordinance (Cap 201).

4. Background of the Project

The DNS protocol can be vulnerable to attack due to an inherent lack of authentication and integrity checking of data that is exchanged between DNS servers or is sent to DNS clients. As originally designed, DNS itself does not offer any form of security and is vulnerable to spoofing and man-in-the-middle attacks. An attacker that has compromised a DNS server can gain access to all network communications that are sent by a targeted host. DNSSEC provides a way to mitigate again this.

DNSSEC includes changes to client and server DNS components that enable DNS data to be cryptographically signed and to enforce name validation policies that protect DNS communications. With DNSSEC, a DNS server can validate responses that it receives as genuine. By validating DNS responses, DNS servers and clients are protected against the single greatest vulnerability in DNS: DNS spoofing.

As the ccTLD for .hk and .香港, HKIRC is charter to provide accurate and secure Domain Name Resolution for these domains and their sub-domain. Hence it is critical that we can provide a DNSSEC supported DNS service.

Currently, HKIRC through it's fully own subsidiary HKDNR provide the following services:

- DNS for .hk and .香港 domain
- Register and registry service for provisioning of new subdomain name

It is the intend of this project to deployment DNSSEC for .hk and .香港 their sub-domain and also to offer this as an additional service to any third level domain.

5. The Required Services

The following defines the scope of service to be provided by the Contractor. There are three parts to the scope:-

- Designing of DNSSEC Solution based on the requirement of 5.1
- Build and implementation of the above solution
- Include first year support for the solution and continuous (renewable) support for the above solution for at least 48 month after the implementation

All vendors should propose for all parts any dependency for any part of the proposal.

5.1. System Requirement

5.1.1 Current Systems:

All services are provided from two Data Centres from two different geographical locations within Hong Kong. There are point to point connections connecting these two Data Centres (100Mbps, Metro Ethernet).

Top-level domain DNS Service:

Top-level domain DNS Service is provided by Open Sources based DNS software. Custom zone file generated from Domain Name registration system which are used to update DNS data. Full zones file generation and update once per day. Real-time Domain modification will update resource records in "stealth" master by nsupdate. Secondary DNS provider get latest zones by standard DNS zone transfer (AXFR/IXFR).

Currently there are multiple zone files of which there are some IDN domains.

Currently there are monitoring in place to monitor the DNS resolution:

- Serial Number checking for all zones
- Dig check on selected VIP domains

Domain Parking Service:

Domain Parking Service is provided by Open Sources based DNS and web server software. Subscriber's domain (must be domain served by above Top-level domain DNS Service)

delegated name servers to HKIRC managed DNS servers which A and AAAA resource records for that domain (and www.) pointed to a HKIRC managed web server which shows a simple webpage. Full zones file generation and update once per 2 hours.

DNS Hosting Service:

DNS Hosting Service is provided by Open Sources based DNS software. Subscriber's domain (must be domain served by above Top-level domain DNS Service) delegated name servers to HKIRC managed DNS servers.

Custom zone file generated from Domain Name registration system which are used to update DNS data. Full zones file generation and update once per day. Real-time Domain modification will update resource records in "stealth" master by nsupdate and rndc. Secondary DNS provider get latest zones by standard DNS zone transfer (AXFR/IXFR) and custom scripts.

HKIRC Internal DNS

Domain Parking Service is provided by Open Sources based DNS. It's to hosting HKIRC internal infrastructure that supports all above services (say DNS to resolve name server names). Domain modification will update resource records in "stealth" master. Secondary DNS provider get latest zones by standard DNS zone transfer (AXFR/IXFR).

Details will be provided on the current system once the tenderee sign the NDA.

5.1.2 General Requirement

a) Tenderer should provide hardware, software licenses and professional services as a total solution. Partial solution offer will NOT be accepted.
b) Tenderer is required to guarantee the hardware model provided in this tender will not be end-of-support by the original at least five (5) years from the delivery date of that hardware.
c) All proposed equipment must be able to function properly and reliably under the following normal Controlled Environmental conditions:
   i. Temperature 10^{o}C to 40 ^{o}C operating
   ii. Humidity 20%-80% non-condensing
d) All hardware proposed should comply with the Electrical Supply Characteristics list below; otherwise the successful tender is required to provide all necessary construction work in the installation site as specified in section 4.5 of this tender:

i. The equipment shall be suitable for use on 220 volts +/- 6% 50Hz single phase
ii. The quality and capacity of all electrical components and cabling shall be fully equivalent to that required by the latest applicable HKSAR Electrical and Mechanical Services Department specifications.
iii. All equipment shall be fitted with 3-core 13A (Live, Neutral, Earth) fused plug for single-phase industrial type supply cable of 3M in length.

e) All proposed features must be demonstrable during tender evaluation or the proposed equipment will not be accepted otherwise.
f) All equipment that has included battery operated component(s) must have a life expectancy of no less than 10 years from the manufacture date.
g) All equipment that has included battery operated component(s) that needed to be replace in regular period shall have manufacturer warranty (battery operation) for at least five years from the date of first use.
h) All equipment that has included battery operated component(s) shall state in the event of battery failure or expire, how the component can be replace. Vendor must provide process and procedure for the replacement of such equipment, without affect the whole of the system.

5.1.3 System Requirement

This project is to provide a solution and its' implementation to HKIRC for:

- DNSSEC for all DNS service mentioned in section 5.1.1 Current Systems.

The solution provided should:

- Adhere to the latest edition following DNSSEC RFC and any referring RFC:
  - 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
- The solution should reference to DNSSEC Practice Statement for the .HK and .香港 top level domain names (HKDPS). Note that the Practice Statement is a draft version and could subject to changes during the project. When value or method is not defined in the HKDPS, the contract should propose value or method according to their implementation experience.
- Integration with HKIRC's existing domain registration system
  - Provide interface with the web interface for DS record input and integrated with the domain registration system
  - Provide an effective method to validate the syntax of DS record inputted by client
  - Zone file validation after signing and chain-of-trust validating from/towards the root
  - Provide system alert if misconfiguration/inconsistencies in the zone are found
- Inline Signer
  - Design and build a DNSSEC inline signing system based on a "bump in the wire" architecture. ie. the DNSSEC zone signing system will sit between our "stealth master" and our DNS authoritative slaves. Zone information is done through bind compatible zone transfer.
  - Support real time zone signing when zone information created, updated and deleted.
  - Support adding/delete zone on the fly without affecting operations.
  - Support DNSSEC algorithms that mentioned in DNSSEC RFCs. (Include but not limited to RSASHA1, RSASHA256, RSASHA1-NSEC3-SHA1, RSASHA512, ECDSAP256SHA256, ECDSAP384SHA384)
  - The signing process should be transparent to both the "stealth master" and the DNS authoritative slaves.
  - The zone signing system should be able to replace by "dropin" replacement, without reconfiguration to "stealth master" nor the DNS authoritative slave.
  - Provide interface to notify on status of the signing process, ie. success or failure
  - Provide a method to validate the KSK and ZSK in all distributed zone after key roll-over
  - Provide traceable logging for all signing process.
  - Provide planning of switch DNSSEC algorithms without affecting operations.
  - Support NSEC and NSEC3 with opt-out, random salt, iterations

- Rational zone/record update signaling to DNS authoritative slave (ie. minimize on notification to DNS authoritative slave).
- Signer should has a minimum performance of:
  - 4000 signed record per second
  - Handle more than one million zones
  - Handle more than one million records per zone
  - Scalable performance with addition hardware within the same box to at least 5 times current performance
- High availability with data replication for key management system as well as DNSSEC signer function include active/passive standby within site and site over different geological location
- Rational handling of Zone file serial number
  - Handle any zone serial number update either transparently or a rational serial numbering scheme.
  - Handle serial number change issue by "stealth master"
- Role based system administration according to DNSSEC Practice Statement of HKIRC including segregation of duty.
- Support full suite of performance and system state/statistic monitoring matrix, eg. CPU loading, RAM usage, zone/record signed, current record per second etc.

- Provide robust and executable disaster recovery facility and procedures to perform emergency recovery actions to resume service within shortest possible time.
- Support Key Management through either HSM or equivalent:
  - Support all key generation standards as stated above RFCs.
  - Support full key lifecycle, ie. create, publication, activation, de-activation and deletion. Please give details in your proposal on how your solution supports the key lifecycle, eg. different key publication method, key generation method, key publication timeline control etc.
  - Support schedulable key lifecycle for KSK and ZSK using both absolute and relative days and actual date.
  - Provide method(s) to perform KSK ceremony.
  - Support schedulable NSEC3 random salt (re)generation.
  - Support secure importing and exporting of keys for backup and restoring.
  - Validated to Security Standard eg. FIPS, RSA, Common Criteria etc.
  - High availability with data replication for key management system, include active/passive failover within site and site over different geological location.
  - Key generation and management according to DNSSEC Practice Statement of HKIRC including segregation of duty.
  - Key generation minimum performance:
    - 4,000 signature per second

        - Scalable performance with addition hardware within the same box to at least 5 times current performance
    - Support full suite of performance and system state/statistic monitoring matrix, eg. CPU loading, RAM usage, signature generated, current signature per second etc.
    - Support secure online/offline storage of keys.
    - Support Emergency Key Rollovers:
        - Support rollover keys out-of-schedule
        - Support emergency regeneration of keys
- Provide process and procedure that does not affect the operation of the system for replacement of any battery operated component that is for:
    - Failure before life expectancy of battery as stated in Section 5.1.2 f)
    - After warranty as stated in Section 5.1.2 g)

5.2. Professional Services

HKDNR is looking for partner that has previous successful experience in implementing DNSSEC solution in ccTLD level. The partner should be able advice on any operation and design consideration for implementing DNSSEC system for .hk and .香港.

The professional services for this Project should cover the following:

- Operational and design advice/recommendation
- Design and build an DNSSEC system based on the requirement of HKDNR
- Procurement and delivery of all system component for this project based on the above design
- Equipment commission service, including equipment mounting, software installation and configuration.
- Interface specification to HKDNR registration system
- Performance benchmarking for proposed system.
- Documentation on design, setup guide and operational/administration procedures including:
    - System design guide
    - System installation and configuration guide
    - System operational/administration guide:
        - Daily operation guide
        - Recurring task guide
        - System Failover/Recovery guide based on different failure mode/scenario, impacts and estimate of Time to Recover.
- Perform complete failover and recovery drill before system commission.
- Preform DNSSEC Infrastructure Audit based on but not limited to DNSSEC Infrastructure

Audit Framework, NLnet Labs Document 2013-002 Version 1.0. Section 4, 5, 6, 8, 9 and 10.

- Deployment plan for system in phases with fallback plan for each phase.
- Support for system during deployment phases (multiple phases). Tentative deployment schedule for HKDNR DNSSEC System are as follows:
  - Phase 1 Signing of .hk and .香港 root zone with IANA. Within nursing period.
  - Phase 2 Signing of zones, eg. .idv.hk, .net.hk etc. Within 3 month from ending of nursing period.
  - Phase 3 Signing of zone, eg. .com.hk, gov.hk. Within 6 month from ending of nursing period.
  - Phase 4 Signing of remaining zones, eg. .org.hk, IDN. Within 9 month from ending of nursing period.
- Nursing period for the system will be 3 month after system goes into production.
- Continuous system support for 12 month after system commission.
- Standby real time failover drill support 6 month after system commission.
- Standby real time for first top and second level KSK key rollover (within 6 month after commission)
- All equipment and service supplied shall come with 24x7 service support contract.

5.3. Information Security

- The Contractor shall follow HKIRC Information Security Policy and Guidelines set out by HKIRC on personal and co-operation data security.
- Contractor's Information Security Policy is subject to HKIRC review if needed.

5.4. Service Acceptance

The overall project acceptance can be broken down into acceptances at various levels:-

1. Delivery, setup of equipment
2. Services provided by professional service
3. Functionality of the integrated system
4. System Performance
5. Documentation, knowledge transfer and training
6. Performance of monitoring system & reporting system
7. Quality of service provided

Under this acceptance framework, the vendor should fulfill the scope of services described in section "The Required Services". In addition, interested vendors may provide additional acceptance criteria and the related plan in detail in their proposals.

5.5. Contractual Consideration

Contract should include all requirements from this RFP. All vendors should propose for all parts of the scope in the RFP. HKIRC reserve the right to take up any part or parts of the each proposal.

5.6. Cost Breakdown

The vendor should breakdown all cost by Capital Expenditure (CapEx) and Operational Expenditure (OpEx). Vendor should justify the cost of OpEx, if it exceeded 10% of CapEx.

6. Limitation of Liability and Indemnity

The company submitting the proposal agrees that if the company becomes the Contractor of the Project, it shall indemnify HKIRC and HKDNR against any claim, demand, loss, damage, cost, expense or liability which the company may suffer from.

7. Information Security

The company submitting the proposal ("the company") shall acknowledge and agree that, if the company is selected as the Contractor, it shall be bounded by our Non-Disclosure Agreement (NDA) and Information Security Policy (highlights of the policies are illustrated in Appendix A). The company shall also comply with the obligations under the Personal Data (Privacy) Ordinance and any other obligations in relation to personal data.

The company shall be provided with a set of NDA and Information Security Compliance Statement after HKIRC received the company's Expression-of-Interest before the stipulated time. The NDA and the Information Security Compliance Statement shall be signed and returned to HKIRC attached with documents required by the Compliance Statement before the scheduled deadline. **HKIRC will only consider proposals from companies which have signed both the NDA and the Information Security Compliance Statement.**

The proposal should be marked "RESTRICTED" at the centre-top of each page in black color. It must be encrypted if transmitted electronically.

Each proposal will be reviewed under the terms of non-disclosure by the HKIRC's staff and Board of Directors of HKIRC.

8. Project Acceptance

The overall project acceptance can be broken down into acceptances at various levels:-

1. Delivery, setup of equipment
2. Services provided by professional service
3. Functionality of the integrated system
4. Performance of monitoring system & reporting system
5. System Acceptance Test
6. User Acceptance Test
7. Documentation, knowledge transfer and training
8. System Failover/Recovery Drill
9. System commissioning
10. Ending of nursing period

9. Anti-collusion

(1) The Tenderer shall not communicate to any person other than HKIRC the amount of any tender, adjust the amount of any tender by arrangement with any other person, make any arrangement with any other person about whether or not he or that other person should or should not tender or otherwise collude with any other person in any manner whatsoever in the tendering process. Any breach of or non-compliance with this sub-clause by the Tenderer shall, without affecting the Tenderer's liability for such breach rules and laws or non-compliance, invalidate his tender.

(2) Sub-clause (1) of this Clause shall have no application to the Tenderer's communications in strict confidence with his own insurers or brokers to obtain an insurance quotation for computation of tender price and communications in strict confidence with his consultants/sub-contractors to solicit their assistance in preparation of tender submission.

(3) The Tenderer shall submit to the HKIRC a duly signed warranty in the form set out in Appendix B to the effect that he understands and will abide by these clauses. The warranty shall be signed by a person authorized to sign the contract on the Tenderer's behalf.

(4) Any breach of any of the representations and/or warranties by the Tenderer may prejudice the Tenderer's future standing as a HKIRC's contractor.

10. Offering Advantages

(1) The Tenderer shall not, and shall procure that his employees, agents and sub-contractors shall not, offer an advantage as defined in the Prevention of Bribery Ordinance, (Cap 201) in connection with the tendering and execution of this contract.

(2) Failure to so procure or any act of offering advantage referred to in (1) above committed by the Tenderer or by an employee, agent or sub-contractor of the Tenderer shall, without affecting the Tenderer's liability for such failure and act, result in his tender being invalidated.

11. Ethical Commitment

11.1. Prevention of bribery

(A) The Contractor shall not, and shall procure that his directors, employees, agents and sub-contractors who are involved in this Contract shall not, except with permission of Hong Kong Internet Registration Corporation Limited (hereafter referred to as the Organisation) solicit or accept any advantage as defined in the Prevention of Bribery Ordinance (Cap 201) in relation to the business of the Organisation. The Contractor shall also caution his directors, employees, agents and sub-contractors against soliciting or accepting any excessive hospitality, entertainment or inducements which would impair their impartiality in relation to the business of the Organisation. The Contractor shall take all necessary measures (including by way of internal guidelines or contractual provisions where appropriate) to ensure that his directors, employees, agents and sub-contractors are aware of the aforesaid prohibition and will not, except with permission of the Organisation, solicit or accept any advantage, excessive hospitality, etc. in relation to the business of the Organisation.

(B) The Contractor shall not, and shall procure that his directors, employees, agents and sub-contractors who are involved in this Contract shall not, offer any advantage to any Board member or staff in relation to the business of the Organisation.

11.2. Declaration of Interest

(C) The Contractor shall require his directors and employees to declare in writing to the Organisation any conflict or potential conflict between their personal/financial interests and their duties in connection with this Contract. In the event that such conflict or potential conflict is disclosed in a declaration, the Contractor shall forthwith take such reasonable measures as are necessary to mitigate as far as possible or remove the conflict or potential conflict so disclosed. The Contractor shall require his agents and sub-contractors to impose similar restriction on their directors and employees by way of a contractual provision.

(D) The Contractor shall prohibit his directors and employees who are involved in this Contract from engaging in any work or employment other than in the performance of this Contract, with or without remuneration, which could create or potentially give rise to a conflict between their personal/financial interests and their duties in connection with this Contract. The Contractor shall require his agents and sub-contractors to impose similar restriction on their directors and employees by way of a contractual provision.

(E) The Contractor shall take all necessary measures (including by way of internal guidelines or contractual provisions where appropriate) to ensure that his directors, employees, agents and sub-contractors who are involved in this Contract are aware of the provisions under the aforesaid sub-clauses (C) and (D).

11.3. Handling of confidential information

(F) The Contractor shall not use or divulge, except for the purpose of this Contract, any information provided by the Organisation in the Contract or in any subsequent correspondence or documentation, or any information obtained when conducting business under this Contract. Any disclosure to any person or agent or sub-contractor for the purpose of the Contract shall be in strict confidence and shall be on a "need to know" basis and extend only so far as may be necessary for the purpose of this Contract. The Contractor shall take all necessary measures (by way of internal guidelines or contractual provisions where appropriate) to ensure that information is not divulged for purposes other than that of this Contract by such person, agent or sub-contractor. The Contractor shall indemnify and keep indemnified the Organisation against all loss, liabilities, damages, costs, legal costs, professional and other expenses of any nature whatsoever the Organisation may suffer, sustain or incur, whether direct or consequential, arising out of or in connection with any breach of the aforesaid non-disclosure provision by the Contractor or his directors, employees, agents or sub-contractors.

11.4. Declaration of ethical commitment

(G) The Contractor shall submit a signed declaration in a form (see Appendix C) prescribed or approved by the Organisation to confirm compliance with the provisions in aforesaid sub-clauses (A) (B), (C), (D), (E) and (F) on prevention of bribery, declaration of interest and confidentiality. If the Contractor fails to submit the declaration as required, the Organisation shall be entitled to withhold payment until such declaration is submitted and the Contractor shall not be entitled to interest in that period. To demonstrate compliance with the aforesaid sub-clauses (A), (B), (C), (D), (E) and (F) on prevention of bribery, declaration of interest and handling of confidential information, the Contractor and the sub-contractors employed for the performance of duties under this Contract are required to deposit with the Organisation a copy of the internal guidelines issued to their staff.

12. Schedule

	Project schedule		
	Tasks	*To be Completed by*	*Remark*
1	Publish RFP	16/3/2015	
2	Express of interest	21/3/2015	
3	Sign NDA and InfoSec Compliance Statement with all interested vendors	21/3/2015	
4	Deadline for vendors to submit proposal and quotation	27/4/2015, 5:30pm	
5	Selection of vendor by panel	5/6/2015	
6	Conclude final decision and appoint the vendor	11/6/2015	
7	Prepare service agreement contract	26/6/2015	
8	Sign service agreement contract with the appointed vendor	10/7/2015	
9	Service implementation	12/10/2015	
10	Service commencement	30/11/2015	
11	Nursing period	29/2/2016	
12	Project Complete	29/2/2016	

13. Payment Schedule

The following payment schedule is recommended but interested vendors may propose their own in their proposals.

	Milestone/Acceptance	**Payment**
1	Delivery of Hardware & Software	40%
2	Hardware & Software Installation Acceptance	10%
3	System performance and SAT/UAT Intergation Acceptance	30%
4	End of nursing period	20%
	TOTAL	**100%**

14. Elements of a Strong Proposal

All submitted proposal must following the format as stated in Appendix D - HKIRC Proposal Requirements

Successful vendor is the one who submitted a clearly worded proposal that demonstrates the following attributes:

- a persuasive section on the company background
- international recognize certification for quality assurance
- a strong and flexible service and tools meeting HKIRC requirements with minimum customization
- high level of interaction between HKIRC and the vendor
- excellent fit with the capabilities and facilities of HKIRC
- strong company and project management team

15. Service Agreement Negotiation and Signature

The service agreement will be drawn up between the selected vendor and HKDNR, the wholly-owned subsidiary of HKIRC. HKIRC welcomes the vendor's proposal on a suitable service agreement for the project/service.

The service agreement must be signed by both parties within one week from the project/service award date. If the agreement is not signed within the said period, HKIRC will start the negotiation with the next qualified vendor on the selection list.

16. HKIRC Contacts

HKIRC Contacts information

Cntacts	
Hong Kong Internet Registration Corporation Limited Unit 2002-2005, 20/F FWD Financial Centre, 308 Des Voeux Road Central, Sheung Wan, Hong Kong +852 23192303 – telephone +852 23192626 – fax http://www.hkirc.hk *If you are not sure about the appropriate person to call, the receptionist can help you.*	**IT Project Manager** Ben Choy +852 23193819 ben.choy@hkirc.hk **Head of IT** Ben Lee +852 23193811 ben.lee@hkirc.hk **CEO** Jonathan Shea +852 23193821 jonathan.shea@hkirc.hk

Appendix A – DNSSEC Practice Statement for the .HK and .香港 top level domain names, Draft

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-draft DNSSEC Policy & Practice Statement Framework (draft-ietf-dnsop-dnssec-dps-framework-04http://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

Document name and identification

Document title: DNSSEC Practice Statement for the .HK and .香港 top level domain names (HK DPS)
Version: 0.1
Created on: 12 March, 2015
Effective on: (TBC)

1.2. Community and Applicability

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

1.2.1. 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.

1.2.2. 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 HKIRC 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.

1.2.3. 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.

1.2.4. 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.

1.2.5. Auditor

Auditor is an entity who audits whether HKIRC DNSSEC Service is operated along with HK DPS or not.

1.2.6. 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 2002-2005, 20/F FWD Financial Centre, 308 Des Voeux Road Central, Sheung Wan, 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 Key Signing Keys 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.

2.3. Access controls on repositories

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

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 Registrant 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. Activation of DNSSEC for child zone

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.

3.4. Registration of Delegation Signer (DS) Resource Records

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) can be registered per domain name.

3.5. 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.

3.6. Registration of delegation signer (DS) resource records

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) can be registered per domain name.

3.6.1. 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.

3.6.2. Procedure for registration request

Registrars are authenticated before using the system interface. Registrars register the DS record(s) to the Registry through the system interface. The Registry will add the DS records in the .HK and .香港 zones.

3.6.3. Emergency registration request

Not applicable.

3.7. 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.

3.8. Removal of DS record

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.

3.8.1. 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.

3.8.2. Procedure for removal request

Registrars are authenticated before they are allowed to use the system interface. Registrars request the removal of DS record(s) to the Registry through the system interface. The Registry will remove the DS records in the .HK and .香港 zones.

3.8.3. Emergency removal request

Not applicable.

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.

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 have begun to generate electricity..

4.1.4. Water exposures

The sites implements water protection and detection mechanisms.

4.1.5. Fire prevention and protection

The sites are equipped with fire detection and extinguishing systems.

4.1.6. Media storage

The Registry's guidelines for information classification define the requirements imposed for the storage of sensitive data.

4.1.7. Waste disposal

Disposed storage media and other material that may contain sensitive information are destroyed in a secure manner, according to the Registry's information security policy.

4.1.8. Off-site backup

Certain critical data is also securely stored using a third-party storage facility. Physical access to the storage facility is limited to authorized personnel. The storage facility is geographically and administratively separated from HKIRC's facilities.

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 generation or use of private keys. The trusted roles are:

1. Systems Administrator, SA
2. Security Officer, SO

4.2.2. Number of persons required per task

At any given time, there must be at least two individuals within the organization per trusted role indicated in 4.2.1.

Key generation requires two people to be present; one from each role.

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

4.2.3. Identification and authentication for each role

Permissions to use the equipment are authorized for each role. Authentication are required before the use of equipment are allowed.

4.2.4. Tasks requiring separation of duties

The trusted roles in 4.2.1 above may not be held simultaneously by one and the same person.

4.3. Personnel Controls

4.3.1. Qualifications, experience, and clearance requirements

Persons who have the trusted roles in 4.2.1 above are limited to full time employees of the Registry.

4.3.2. Background check procedures

The evaluation of background checks is conducted by the HR function at HKIRC.

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. Retraining frequency and requirements

The Registry provides trainings as necessary, such as when there is major change in the operation, systems and organization.

4.3.5. Job rotation frequency and sequence

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

4.3.6. Sanctions for unauthorized actions

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

4.3.7. Contracting personnel requirements

In certain circumstances, HKIRC may need to use contractors as a supplement to full-time employees. These contractors are managed according to the HKIRC's Information Security Policy.

4.3.8. 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 following events are included in logging:

- Key management activities, such as key generation, key activation, and signing and exporting keys.
- Remote access, successful and unsuccessful.
- Privileged operations.
- Entry to a facility.

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 30 days.

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

Not applicable.

4.4.7. Notification to event-causing subject

Not applicable.

4.4.8. Vulnerability assessments

All anomalies in the log information are investigated to analyze potential vulnerabilities.

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.

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

The key generation takes place in signing systems managed by trained personnel in trusted roles. Key generation takes place when necessary and is performed by two personnel simultaneously.

5.1.2. Public key delivery

The public component of each generated KSK is exported from the signing system and verified by the SO and SA. The SO is responsible for publishing the public component of the KSK in a secure manner. The SA is responsible for ensuring that the keys that are published are the same as those that were generated.

5.1.3. Public key parameters generation and quality checking

The Registry periodically confirms that generation of signing key is conducted with appropriate parameters and is with the correct key length.

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

TBC

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

The Registry does not apply multi-person controls of the private keys.

5.2.3. Private key escrow

The Registry does not apply a key escrow.

5.2.4. Private key backup

The private key are backup into separate signing systems that are installed in the protected facilities.

5.2.5. Private key storage on cryptographic module

TBC.

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

The key will be stored in an encrypted form in a portable media when a transfer is needed.

5.2.8. Method of activating private key

TBC. Depends on Key Management System.

5.2.9. Method of deactivating private key

TBC. Depends on Key Management System

5.2.10. Method of destroying private key

Private keys are not destructed. After their useful life, they are removed from the signing system.

5.3. Other Aspects of Key Pair Management

5.3.1. Public key archival

Public keys are not archived.

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. 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 (passphrase) according to the requirements set out in the Registry's Information Security Policy.

5.4.2. Activation data protection

Each personnel is responsible for protecting their activation data in the best reasonable possible way. On the suspicion of compromised activation data, 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. Logging is conducted in the firewalls. Transmission of classified information is protected with suitable method (e.g. encryption) according to the Registry's Information Security Policy.

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 adopted an Information Security Policy. 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 Registry has adopted an Information Security Policy. 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

The key types of signing keys of the HK zone are KSK and ZSK.

The key length of KSK is 2048 bits and that of ZSK is 1024 bits (Tentative, subject to change) but other key length should be supported.

The algorithm for both KSK and ZSK is RSASHA256 (Tentative, subject to change) but other algorithms (include but not limited to RSASHA1, RSASHA256, RSASHA1-NSEC3-SHA1, RSASHA512, ECDSAP256SHA256, ECDSAP384SHA384) should be supported.

NSEC3 Salt length at least 64 bit.

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 described in RFC 4641.

6.4.2. Key signing key roll-over

KSK rollover is carried out on an annual basis by the double signature method described in RFC 4641.

6.5. Signature Validity Period and Re-signing Frequency

RR sets are signed with KSKs with validity period of = 15 days (Tentative, subject to change)
RR sets are signed with ZSKs with validity period of = 15 days (Tentative, subject to change)

Resigning frequency using KSKs is = 1 year
Resigning frequency using ZSKs is = 1 month

These values are for reference only and may be changed without prior notice.

6.6. Verification of zone signing key set

To ensure signatures and the validity period of keys, security controls are conducted against the DNSKEY prior to publishing zone information on the Internet. This is done by verifying the chain from DS in the parent zone to KSK, ZSK and the signature over the zones SOA.

6.7. Verification of resource records

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

6.8. Resource records time-to-live

DNSKEY = 28800, i.e. 8 hours
NSEC3 and NSEC3PARAM = negative cache value = now is 600 sec, i.e. 10 mins
RRSIG of NSEC3 = negative cache value = now is 600 sec, i.e. 10 mins

DS = NS TTL = 28800 (Tentative, subject to change)
RRSIG of DS = DS's TTL
RRSIG = inherits TTL from the RRset = 28800 (Tentative, subject to change)

These values are for reference only and may be changed without prior notice.

7. COMPLIANCE AUDIT

7.1. Frequency of entity compliance audit

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

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

HK 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 HKIRC 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.

.

Appendix B – HKDNR Information Security Policy and Guidelines: An Extract Relevant to Outsourcing

This document provides an extract of the HKDNR Information Security Policy and Guidelines with the purposes of (a) introducing various measures and controls to be executed by HKDNR regarding outsourcing and (b) setting the expectation of any potential contractors that their participation and conformance in these measures and controls are essential contractual obligations.

The original Policy and Guidelines applies to HKDNR's employees, contractors and third party users. However, a potential contractor may interpret the clauses up to their roles and responsibilities only. Nonetheless, the keyword "**contractors**" hereby refers to all relevant staff members of the contractor and those of any other subcontractors under the contractor's purview.

Herein, HKDNR would also set the expectation of any potential contractors that upon their expression-of-interest to the project/service, they shall be required in the subsequent stages (a) to sign off a non-disclosure agreement (NDA) on all information to be provided and (b) to sign off a Compliance Statement where compliance requirements are specified in more details.

(A) Extract from the HKDNR Information Security Policy

In the following, "the organization" means Hong Kong Domain Name Registration Company Limited, the company requesting the proposal for "the Project."

8. Human resources security

8.1 Security objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

8.1.1 Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.

8.1.2 Background verification checks on all candidates for employment, contractors, and third

party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

8.1.3 As part of their contractual obligations, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.

8.2 During employment

Security objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

8.2.1 Management shall require employees, contractors and third party users to apply security measures in accordance with established policies and procedures of the organization.

8.2.2 All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates on organizational policies and procedures, as relevant to their job functions.

8.3 Termination or change of employment

Security objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

8.3.2 All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.

8.3.3 The access rights of all employees, contractors and third party users to information and information processing facilities shall either be removed upon termination of their employment, contract or agreement, or adjusted upon change.

12. Information systems acquisition, development and maintenance

12.5.5 Outsourced software development shall be supervised and monitored by the organization

13. Information security incident management

13.1 Reporting information security events and weaknesses

Security objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action.

13.1.2 All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

(B) Extract from the HKDNR Information Security Guidelines

6. ORGANIZING INFORMATION SECURITY

6.2 EXTERNAL PARTIES

6.2.1 Identification of Risks Related to External Parties

The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting the access.

6.2.3 Addressing Security in Third Party Agreements

Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.

7. ASSET MANAGMENT

7.1.3 Acceptable Use of Assets

Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.

8. HUMAN RESOURCE SECURITY

8.1.1 Roles and Responsibilities

Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.

8.1.2 Screening

Background verification checks on all candidates for employment, contractors, and third party users shall be conducted in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

8.1.3 Terms and Conditions of Employment

As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.

8.2.1 Management Responsibilities

Management shall require employees, contractors and third party users to apply security measures in accordance with established policies and procedures of the organization.

12. Information systems acquisition, development and maintenance

12.5.5 Outsourced Software Development

Outsourced software development shall be supervised and monitored by the organization.

Appendix C – Warranty

[start in next page]

To: Hong Kong Internet Registration Corporation Limited (HKIRC)

Dear Sir/Madam,

Warranty

(1) By submitting a tender, the Tenderer represents and warrants that in relation to the tender of Domain Name System Security Extensions (DNSSEC)" Implementation Project:

(i) it has not communicated and will not communicate to any person other than the HKIRC the amount of any tender price;

(ii) it has not fixed and will not fix the amount of any tender price by arrangement with any person;

(iii) it has not made and will not make any arrangement with any person as to whether it or that other person will or will not submit a tender; and

(iv) it has not otherwise colluded and will not otherwise collude with any person in any manner whatsoever in the tendering process.

(2) In the event that the Tenderer is in breach of any of the representations and/or warranties in Clause (1) above, the HKIRC shall be entitled to, without compensation to any person or liability on the part of the HKIRC :

(i) reject the tender;

(ii) if the HKIRC has accepted the tender, withdraw its acceptance of the tender; and

(iii) if the HKIRC has entered into the contract with the Tenderer,

terminate the contract.

(3) The Tenderer shall indemnify and keep indemnified the HKIRC against all losses, damages, costs or expenses arising out of or in relation to any breach of any of the representations and/or warranties in Clause (1) above.

(4) Clause (1) shall have no application to the Tenderer's communications in strict confidence with its own insurers or brokers to obtain an insurance quotation for computation of the tender price, or with its professional advisers, and consultants or sub-contractors to solicit their assistance in preparation of tender submission. For the avoidance of doubt, the making of a bid by a bidder to the HKIRC in public during an auction will not by itself be regarded as a breach of the representation and warranty in Clause (1)(i) above.

(5) The rights of HKIRC under Clauses (2) to (4) above are in addition to and without prejudice to any other rights or remedies available to it against the Tenderer.

Authorized Signature & Company Chop :

Name of Person Authorized to Sign (in Block Letters) :

Name of Tenderer in English (in Block Letters) :

Date :

Appendix D – Declaration Form by Contractor on their compliance with the ethical commitment requirements

[start in next page]

To: Hong Kong Internet Registration Corporation Limited (HKIRC)
Contract No.:
Title:

In accordance with the Ethical Commitment clauses in the Contract:

1) We confirm that we have complied with the following provisions and have ensured that our directors, employees, agents and sub-contractors are aware of the following provisions:

   a) prohibiting our directors, employees, agents and sub-contractors who are involved in this Contract from offering, soliciting or accepting any advantage as defined in section 2 of the Prevention of Bribery Ordinance (Cap 201) in relation to the business of HKIRC except with the permission of HKIRC;

   b) requiring our directors, employees, agents and sub-contractors who are involved in this Contract to declare in writing to their respective company management any conflict or potential conflict between their personal/financial interests and their duties in connection with this Contract, and in the event that a conflict or potential conflict is disclosed, take such reasonable measures as are necessary to mitigate as far as possible or remove the conflict or potential conflict so disclosed;

   c) prohibiting our directors and employees who are involved in this Contract from engaging in any work or employment (other than in the performance of this Contract), with or without remuneration, which could create or potentially give rise to a conflict between their personal/financial interests and their duties in connection with this Contract and requiring our agents and sub-contractors to do the same; and

   d) taking all measures as necessary to protect any confidential/privileged information or data entrusted to us by or on behalf of HKIRC from being divulged to a third party other than those allowed in this Contract.

Signature
(Name of the Contractor)
(Name of the Signatory)
(Position of the Signatory)
(Date)

Appendix E – HKIRC Proposal Requirements

Proposal requirements	
Submission deadline	Please refer to Section 12 - Schedule, item no. 4 for the proposal submission deadline. If tropical cyclone warning signal No.8 or above or the black rainstorm warning is hoisted on the deadline date, the deadline will be postponed to the next working day without advance notice.
Delivery address	Hong Kong Internet Registration Corporation Limited Unit 2002-2005, 20/F , FWD Financial Centre 308 Des Voeux Road Central, Sheung Wan, Hong Kong
Hard copies	2 copies of the full proposal are required. The proposal shall be to the attention of Elisa Chung (Senior Finance Officer) or Bonnie Chun (Head of Operations)
Electronic copy	Electronic copy is required, on disk or by email to elisa.chung@hkirc.hk and bonnie.chun@hkirc.hk; also cc ben.choy@hkirc.hk and ben.lee@hkirc.hk. This is not a substitute for the physical copies mentioned above.
Proposal format	Specified in this document
Page count	30 pages or fewer. Stapled. Do not bind.
Font	Electronically published or typed. Times New Roman 12 point font.

1.2 Proposal Content

The proposal should contain the following:

- Cover Page
- Executive Summary
- Conflict of Interest Declaration
- Company Background
    - Financial Situation
    - Track Records
    - Organization and management team
    - Project team with credentials
    - Company credentials
    - Staff credentials
- Methodology
- Project management methodology
- Understanding of our requirements
- Knowledge and Advices on Projects/Services
- Deliverable and Services level
- Proposed Cost of Services and Payment Schedule
- Implementation Time Table
- Commercial and Payment Terms. e.g. Compensation for delay.

1.3 Cover Page

Prepare a non-confidential cover page with the following information in the order given.

Cover Page		
Project Title		
		Domain Name System Security Extensions (DNSSEC) Implementation Project
Project Manager	Name:	
	Title:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
Company	Contact person:	
	Title:	
	Company name:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
	Website:	

1.4 Executive Summary

The executive summary provides a brief synopsis of the commercial and technical solution the vendor proposed for the project/service. This summary must be non-confidential. It should fit on a single page.

The executive summary should be constructed to reflect the merits of the proposal and its feasibility. It should also clearly specify the project/service's goals and resource requirements. It should include:

- Rationale for pursuing the project or service, the methodology/technology needed and the present state of the relevant methodology/technology.
- Brief description of the vendor's financial situation.
- Brief description of the vendor's facilities and experience on similar projects or services

1.5 Conflict of Interest Declaration

Declare any conflict of interest in relation to the project and the '.hk' ccTLD registry HKIRC.

1.6 Company Background

The vendor must describe its company background. Major activities, financial situation, organizational structure, management team and achievements in similar projects/services or service outsourcing of the company should be elaborated. Track records are preferred.

List the key technical and management personnel in the proposal. Provide a summary of the qualifications and role of each key member.

1.7 Methodology

The vendor must describe the methods to be used, and briefly explains its advantage and disadvantage. Track records are preferred.

1.8 Project Management Methodology

The vendor must describe the methods to be used, and briefly explains its advantage and disadvantage. Track records are preferred.

1.9 Understanding of our requirements

The vendor shall describe their understanding of our requirements. With the use of a table, the vendor should clearly state their compliance on the requirements listed in the scope of service section; and briefly explain how they are achieved.

1.10 Knowledge and Advices on Projects/Services

The vendor should describe their knowledge and advices to ensure the success of this

project/service or projects/services with similar nature.

1.11 Deliverable and Services level

The vendor should detail the project/service deliverables, and the services level of the proposed services. Tables of content of all reports included in the deliverables should be provided in the proposal.

1.12 Proposed Costs of Service and Payment Schedule

The vendor should provide the breakdown of the cost of the whole project/service. The cost shall be broken down by milestone/phases. The payment shall be scheduled based on the milestones and/or deliverables.

Such costs should include, if applicable:

- Fixed setup cost
- Labour unit costs for additional services or requirements. They are typically quoted in unit man day. Quoted in normal working hour, non-working hour and in emergency.
- Equipment that is permanently placed or purchased for HKIRC to complete the project or service, if any.
- Subsequent support, maintenance or consultation service.
- Other direct costs including services, materials, supplies, postage, traveling, pocket money, etc.

1.13 Implementation Time Table

The vendor should present in this section the implementation schedule of the project/service. The schedule should be realistic and achievable by the vendor.

1.14 Commercial and Payment Terms

The vendor should describe the commercial and payment terms of the services e.g. compensation for the delay of the project/service.