Recognized Certification Authority (RCA) and WebTrust Audit

Request for Proposal

(Tender Ref.: RFP-DCERT-RCA-WT-01)

Version 2.0
Date: 29 August 2025

Hong Kong Internet Registration Corporation Limited

Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong
Tel.: +852 2319 1313 Fax: +852 2319 2626
Email: enquiry@hkirc.hk Website: www.hkirc.hk

IMPORTANT NOTICE

This communication contains information which is confidential and may also be privileged. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s), please note that any distribution, copying or use of this communication or the information in it is strictly prohibited. If you have received this communication in error, please notify the sender immediately and then destroy any copies of it.

Table of Contents

Summary 5
1. Definitions 6
2. About HKIRC 7
3. Background of the Project 8
4. The Required Services and System Functionalities 9
4.1. Recognized Certification Authority (RCA) and WebTrust Audit 9
5. Limitation of Liability and Indemnity 14
5.1. Service Level Agreement (SLA), Service Credits and Contract Termination 14
5.2. Project Management Methodology and Review Meeting 15
5.3. Intellectual Property Rights 15
5.4. Software Source Code Escrow 15
6. Information Security 15
7. Project Acceptance 16
8. Anti-collusion 16
9. Offering Advantages 17
10. Compliance with law 17
11. Ethical Commitment 17
11.1. Prevention of bribery 17
11.2. Declaration of Interest 18
11.3. Handling of confidential information 18
11.4. Declaration of ethical commitment 19
12. Time Schedule 20
13. Payment Schedule 22
14. Elements of a Strong Tender 22
15. Service Agreement Negotiation and Signature 23
16. HKIRC Contacts 24
Appendix A – Warranty 25
Appendix B – Declaration Form by Contractor on their compliance with the ethical commitment requirements 28
Appendix C – HKIRC Proposal Requirements 30
1 Proposal Content 31
2 Cover Page 32
3 Executive Summary 33
4 Conflict of Interest Declaration 33
5 Company Background 33
6 Audit Approach and Methodology 33
7 Project Management Methodology 33

8 Understanding of our requirements....33
9 Knowledge and Advices on Projects/Services....33
10 Deliverable and Services level....34
11 Proposed Costs of Service and Payment Schedule....34
12 Implementation Time Table....34
13 Commercial and Payment Terms....34
Appendix D – HKIRC Information Security Policy: An Extract Relevant to Outsourcing....35
7. HUMAN RESOURCES SECURITY....35

Summary

Hong Kong Internet Registration Corporation Limited (HKIRC) is going to commission a Service Provider ("the Contractor") to conduct Recognized Certification Authority (RCA) and WebTrust audit for our Certification Authority.

The scope of services and requirements are detailed in Section 4 of this document.

Parties interested in providing this service should **sign Non-disclosure Agreement (NDA) by 2nd September 2025** and **submit proposal** (see Appendix C) to the Group **no later than 5:00pm on 5th September 2025 (Hong Kong time)**.

The Contractor should submit Proposal by email to HKIRC contacts (refer to Appendix C - HKIRC Proposal Requirements, electronic copy). The Contractor must provide their information as required in the proposal cover page (Appendix C, 2 Cover Page).

1. Definitions

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

“The Contractor” and “The Service Provider” mean the company who will provide the Services after award of contract.

“HKIRC” means Hong Kong Internet Registration Corporation Limited, the company requesting the proposal for “The Services”.

“HKDNR” means Hong Kong Domain Name Registration Company Limited, a wholly-owned subsidiary of HKIRC.

“CA” and “Certification Authority” mean the body issuing digital certificates, i.e. HKIRC.

“The Certificate(s)” and “Digital Certificate(s)” mean the digital certificates to be issued by the Certification Authority in this Project.

“The Infrastructure” and “CA Infrastructure” mean Certification Authority infrastructure. It consists of the CA System, server infrastructure and secure facilities.

“The System” and “CA System” mean Certification Authority system. It consists of a web application for certificate subscription/ issuance, integration with DNRS for offering SSL certificate, and other components for certificate issuance.

“The Services” and “The Project” mean the Recognized Certification Authority (RCA) and WebTrust Audit according to the requirements stipulated in Section 4 of this document.

“RFP” means this Request for Proposal.

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

2. 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 endeavors 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 https://www.hkirc.hk .

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

3. Background of the Project

Hong Kong Internet Registration Corporation Limited (HKIRC) is establishing a new certification authority (CA) that will provide reliable and secure digital certificates to organizations and individuals. The certification authority will be responsible for verifying the identities of certificate subscribers and issuing digital certificates that can be used to encrypt and authenticate online communications.

The CA targets to issue the digital certificates, including but not limited to:

1. Personal
2. Organizational
3. Encipherment
4. Server (including Domain Validation (DV), Organization Validation (OV) and Extended Validation (EV) certificates)
5. Governmental
6. Organizational Role
7. Bank
8. "iAM Smart"
9. Digital Corporate Identity platform "CorpID"

HKIRC will establish the certification authority (CA) infrastructure, including hardware, software, server infrastructure and secure facilities, etc., which must support HKIRC to become a Recognized Certification Authority (RCA) under ETO[1], COP[2] and CPS(s)[3]. For offering SSL certificates to our customers, the CA System will be fully integrated with our Domain Name Registration System (DNRS).

In this Project, the Service Provider has to conduct Recognized Certification Authority (RCA) and WebTrust audit for HKIRC to be accredited as a Recognized Certification Authority; and to obtain trust from common web browsers.

[1] ETO - the Electronic Transactions Ordinance (Cap. 553)

[2] COP - the Code of Practice for Recognized Certification Authorities published by the Commissioner for Digital Policy pursuant to section 33 of the ETO

[3] CPS - Certification Practice Statement - a statement issued by HKIRC CA to specify the practices and standards that the HKIRC CA employs in issuing Certificates

4. The Required Services and System Functionalities

The following defines the scope of service to be provided by the Contractor. The scope of service consists of the following parts, and the high-level requirements are stated below:-

- Recognized Certification Authority (RCA) audit (optional)
- WebTrust audit (optional)

Tenderers can offer either RCA audit or WebTrust audit or both audits, and must separate into 2 offers for RCA audit and WebTrust audit respectively; and provide quotation breakdown for each item in their proposals for our consideration. Please refer to **Section 11 Proposed Costs of Service and Payment Schedule** of **Appendix C – HKIRC Proposal Requirements** for the items and breakdown required. Tenderers' offers have to remain valid for at least 6 months from the RFP closing date. HKIRC reserves the right to award the RFP for accepting partial or the whole proposal by Tenderer(s), including but not limited to either RCA audit or WebTrust audit or both audits.

4.1. Recognized Certification Authority (RCA) and WebTrust Audit

HKIRC would like to serve as a Recognized Certification Authority (RCA) in accordance with the Electronic Transaction Ordinance (Cap. 553) (ETO), the Code of Practice for Recognized Certification Authorities (COP) and Certificate Practice Statement (CPS). For the details of RCA, please refer to the website of Digital Policy Office (DPO) (https://www.digitalpolicy.gov.hk/en/our_work/digital_infrastructure/legal_framework/regulation/eto/ca/recognition_of_ca_and_cert/). The Certification Authority (CA) Infrastructure built by the Service Provider must comply with the requirements of RCA. During the application for being recognized as RCA.

In this RCA project, we target to issue the following recognized certificates, which are also listed in the website of DPO (https://www.digitalpolicy.gov.hk/en/our_work/digital_infrastructure/legal_framework/regulation/eto/digital_cert/types_of_digital_cert/):

Types of Recognized Digital Certificates	Types of Users	Main Purposes of Use
Personal	Individuals	To conduct secure message transmissions as well as electronic transactions by means of encryption/decryption and digital signing to prove their identity to third parties
Organisational	Staff of Organisations	To conduct secure message transmissions as well as electronic transactions by means of encryption/decryption and digital signing for and on behalf of their organisations
Encipherment	Units of the Organisation	To conduct secure message transmissions by means of encryption/decryption
Server	Single or Multiple Servers / Web sites of Organisations	To verify the identity of web site(s) to the client browser and communicate in Secure Socket Layer (SSL) messages
Governmental	Staff of Government bureau / departments	To conduct secure message transmissions as well as electronic transactions by means of encryption/decryption and digital signing for and on behalf of the bureaux/departments used for the purposes as designated by their bureaux/departments
Organisational Role	Staff of Organisations	To conduct secure message transmissions as well as electronic transactions by means of encryption/decryption and digital signing for and on behalf of their role in the

Bank	Personal / Corporate / Bank	To create digital signature on e-Cheque
"iAM Smart"	Hong Kong residents	To conduct digital signing via the "iAM Smart" system to handle statutory documents and procedures
"CorpID"	Organisations	To conduct authentication of identity of enterprises via Digital Corporate Identity platform ("CorpID")

In accordance with Section 20(3)(b) of the Electronic Transactions Ordinance (Cap. 553) ("ETO"), the Certification Authority setup by HKIRC ("HKIRC CA") shall submit to the Commissioner for Digital Policy ("CDP") a report containing an assessment as to whether the HKIRC CA is capable of complying with such provisions of the ETO and of the Code of Practice for Recognized Certification Authorities ("COP") as are specified in the COP (such provisions are specified under paragraph 1 of Appendix 2 of the COP).

Tenderer must acknowledge and agree that the HKIRC CA shall apply to the CDP for approval that the tenderer whom the HKIRC CA intends to engage for the preparation of an assessment report under section 20(3)(b) of the ETO is a qualified person, and furnish the CDP with the required documents and information in respect of the application. Qualifications of the person are set out in section 12 of the Code of Practice.

Tenderers are required to submit the documents and information required for application to engage a qualified person under the ETO at the following URL published by DPO: - https://www.digitalpolicy.gov.hk/en/our_work/digital_infrastructure/legal_framework/regulation/eto/doc/app_assessor.pdf

To prepare such assessment report, the qualified person must follow the Guidance Note on Compliance Assessment of Certification Authorities: - https://www.digitalpolicy.gov.hk/en/our_work/digital_infrastructure/legal_framework/regulation/eto/doc/guide_assess.pdf

Additionally, although HKIRC CA is not currently a member of CA/Browser Forum[4], we have pledged to adhere to the baseline requirements for the Issuance and Management of Publicly-Trusted Certificates (SSL/TLS server certificates) criteria established by the CA/Browser Forum (currently at v2.1.4 or the latest version), in relations to the issuance and management of the server certificates for HKIRC CA. The qualified person (i.e. the qualified assessor) will assist HKIRC CA (with Certizen acting as its agent) in preparing an independent assessment report, with reference to WebTrust for CA (currently v2.2.2 or the latest version), WebTrust for CA - SSL Baseline (currently at v2.8 or the latest version)，WebTrust for CA - Network Security (currently at v1.7 or the latest version), and WebTrust for CA – Extended Validation SSL (currently at v1.8 or the latest version) on its current status in respect of the above baseline requirements.

Against the background as described in the paragraphs above, the scope of service will cover the following areas:

MANDATORY REQUIREMENTS

1) Independent Assessment of the HKIRC as a RCA under section 20(3)(b) of the ETO, including the Certificate Policy for Mutual Recognition of Electronic Signature Certificates issued by Hong Kong and Guangdong ("MRCP").
2) Conduct an assessment and issue a point-in-time assessment report in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities version 2.2.2, or the latest version, during the HKIRC's Root CAs and Subordinate CAs key generation process, which will be scheduled for a specific date.
3) While conducting the independent assessment outlined in item 1, the assessor is required to conduct an assessment and issue a point-in-time assessment report in accordance with the following WebTrust Principles and Criteria:
    a. WebTrust Principles and Criteria for Certification Authorities ("WebTrust for CA") version 2.2.2 or later;
    b. WebTrust Principles and Criteria for Certification Authorities – SSL Baseline ("WebTrust for CA – SSL BR") version 2.8 or later;
    c. WebTrust Principles and Criteria for Certification Authorities - Network Security ("WebTrust for CA - Network Security") version 1.7 or later; and
    d. WebTrust for Certification Authorities – Extended Validation SSL ("WebTrust for CA – EV SSL") version 1.8 or later.

[4] The CA/Browser Forum is a voluntary organization of Certification Authorities and suppliers of Internet browser and other relying-party software applications. As such, it continually publishes guidelines on best practice and standards for the CA industry and community to improve the trustworthiness of publicly trusted certificates.

4) After 6 months from the issuance of the assessment report for item 3, the assessor is required to conduct an audit and issue a period-of-time audit report covering a period of at least 180 calendar days, in accordance with the following WebTrust Principles and Criteria:
    a. WebTrust Principles and Criteria for Certification Authorities ("WebTrust for CA") version 2.2.2 or later;
    b. WebTrust Principles and Criteria for Certification Authorities – SSL Baseline ("WebTrust for CA – SSL BR") version 2.8 or later;
    c. WebTrust Principles and Criteria for Certification Authorities - Network Security ("WebTrust for CA - Network Security") version 1.7 or later; and
    d. WebTrust for Certification Authorities – Extended Validation SSL ("WebTrust for CA – EV SSL") version 1.8 or later.
5) After finalizing the WebTrust audit reports outlined in item 4, submit an application to CPA Canada for the WebTrust Seal.

OPTIONAL REQUIREMENTS

6) During the course of the aforementioned engagements, providing reports with reference to the latest version of the Practice Guide for Security Risk Assessment and Audit Guidelines issued by the DPO and other guidelines as provided by HKIRC.

5. Limitation of Liability and Indemnity

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

5.1. Service Level Agreement (SLA), Service Credits and Contract Termination

All services provided by the Service Provider shall be sized and scaled to meet the agreed SLA, including but not limited to implementing the Project according to the agreed project schedule without significant deviation; delivering project deliverables up to industrial standards and quality levels; protecting data integrity and confidentially; and maintaining system availability at the agreed level. All planned activities which would affect the Production environment and daily operations shall be notified to and agreed with HKIRC four weeks in advance.

In case of the Service Provider's service level does not meet with the proposed SLA, the Service Provider shall, as part of the SLA, include a Service Credit scheme or any applicable remedial actions (at the Service Provider's own cost) for compensation for the service which did not meet the SLA. Service Provider may propose detail scheme during the contractual negotiation stage, but will need to outline the proposed scheme within the tender for HKIRC to evaluate.

In the event of any project delay with respect to a Project Milestone, HKIRC shall be entitled to service credits (in terms of man-days) equivalent to (a) the percentage of Project delay (i.e. number of months of delay divided by overall Project duration) times (b) the Project Sum divided by (c) the higher of (i) the Service Provider's man-day rate to HKIRC at the time of the delay or (ii) a man-day rate mutually agreed (the "Service Credits").

HKIRC also reserves the right to terminate the contract based on a "3-strike" principle; the Service Provider shall not break the SLA for more than three times during the project period. HKIRC also reserves the right to terminate the service if the service provided:

- Causes disruption and/or losses to HKIRC business and operation.
- Causes service downtime without notices.

5.2. Project Management Methodology and Review Meeting

Please propose the project management methodology the Service Provider would adopt for governing the implementation of the Project. Review meetings, on monthly basis, should be arranged for the purposes including but not limited to:

- Monitor and review the overall project progress, quality of project deliverables.
- Discuss and propose action plans for any project-level issues.
- Manage any project-related risks and incidents.

5.3. Intellectual Property Rights

The Service Provider's proposed solution, and its components, shall not infringe the intellectual property rights of any third party. The Service Provider shall bear the liability or consequence for any intellectual property rights infringement made by the Service Provider and/or in its solution for the Project.

5.4. Software Source Code Escrow

It is required to use open source frameworks for the development of the System and release the source code to HKIRC/ HKDNR without additional cost incurred. If this arrangement cannot be made, the Service Provider is required to make software source code escrow arrangement to allow HKIRC/ HKDNR to retrieve and use the software source code of the System for any circumstances in which the Service Provider no longer supports and maintains its solution.

6. 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 D). 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 after HKIRC received the company's Expression-of-Interest before the stipulated time. The NDA shall be signed and returned to HKIRC before the scheduled deadline. HKIRC will only consider proposals from companies which have signed the NDA.

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.

7. Project Acceptance

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

1. Issuance of the report of assessment of the HKIRC as a RCA under section 20(3)(b) of the ETO
2. Issuance of the point-in-time assessment report on CA Key Generation (Criterion 4.1 of the WebTrust for CA).
3. Issuance of the point-in-time assessment report on WebTrust for CA, WebTrust for CA – SSL BR, WebTrust for CA – Network Security and WebTrust for CA – EV SSL.
4. Issuance of the period-of-time assessment report on WebTrust for CA, WebTrust for CA – SSL BR, WebTrust for CA – Network Security and WebTrust for CA – EV SSL.
5. Application for the WebTrust Seal.

8. 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 A 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.

9. 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.

10. Compliance with law

Notwithstanding anything to the contrary under the Agreement of this Project, HKIRC reserves the right to disqualify the Service Provider on the grounds that the Service Provider has engaged, is engaging, or is reasonably believed to have engaged or be engaging in acts or activities that are likely to cause or constitute the occurrence of offences endangering national security or otherwise the exclusion is necessary in the interest of national security, or is necessary to protect the public interest of Hong Kong, public morals, public order or public safety.

HKIRC may immediately terminate the Agreement of this Project upon the occurrence of any of the following events:
(a) the Service Provider has engaged or is engaging in acts or activities that are likely to constitute or cause the occurrence of offences endangering national security or which would otherwise be contrary to the interest of national security; or
(b) the continued engagement of the Service Provider or the continued performance of the Services is contrary to the interest of national security; or
(c) HKIRC reasonably believes that any of the events mentioned above is about to occur.

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 B) 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. Time Schedule

	Tasks	To be Completed by
1	Publish RFP	29-Aug-2025
2	Sign Non-disclosure Agreement (NDA)	2-Sep-2025
3	Deadline for vendors to submit proposal	5-Sep-2025, 5:00pm
4	Sign service agreement contract with the appointed vendor	September 2025
5	Kick-start of the project	Before 1 October 2025
6	Project completion	July 2026

The Service Provider shall assign a team of competent audit staffs to commence field audit no later than 17 October 2025 or whatever time to be discussed with HKIRC CA in order to meet the target to complete the duly signed audited reports according to the following schedule.

	Task	Field Audit Completed by	Draft Report Issued by	Final Report Issued by
1	An independent assessment in accordance with S.20(b) of the ETO	December 2025	12 December 2025	2 January 2026
2	An independent assessment in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities version 2.2.2, or the latest version	A specific date in October 2025	31 October 2025	7 November 2025
3	Point-in-Time Assessment WebTrust for CA	December 2025	12 December 2025	2 January 2026
4	Point-in-Time Assessment WebTrust for CA – SSL BR	December 2025	12 December 2025	2 January 2026

	Task	Field Audit Completed by	Draft Report Issued by	Final Report Issued by
5	Point-in-Time Assessment WebTrust for CA - Network Security	December 2025	12 December 2025	2 January 2026
6	Point-in-Time Assessment WebTrust for CA - EV SSL	December 2025	12 December 2025	2 January 2026
7	Period-of-Time Audit WebTrust for CA	June 2026	17 July 2026	31 July 2026
8	Period-of-Time Audit WebTrust for CA – SSL BR	June 2026	17 July 2026	31 July 2026
9	Period-of-Time Audit WebTrust for CA - Network Security	June 2026	17 July 2026	31 July 2026
10	Period-of-Time Audit WebTrust for CA - EV SSL	June 2026	17 July 2026	31 July 2026

13. Payment Schedule

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

For RCA audit:

Milestone	Items	Payment
1.	Acceptance of project plan	30%
2.	Upon issuance of the assessment report on HKIRC as an RCA under Section 20(3)(b) of the ETO.	70%

For WebTrust audit:

Milestone	Items	Payment
1.	Acceptance of project plan	30%
2.	Upon issuance of the point-in-time assessment report on CA Key Generation (Criterion 4.1 of WebTrust for CAs).	23%
3.	Upon issuance of the point-in-time assessment report on WebTrust for CA, WebTrust for CA — SSL BR, WebTrust for CA — Network Security, and WebTrust for CA — EV SSL.	23%
4.	Upon issuance of the period-of-time assessment report on WebTrust for CA, WebTrust for CA — SSL BR, WebTrust for CA — Network Security, and WebTrust for CA — EV SSL.	24%

If the WebTrust has been passed and is ready for WebTrust Seal Application, the auditor has to submit the WebTrust Seal Application, and the application fee will be paid on actual basis.

14. Elements of a Strong Tender

All submitted tender must follow the format as stated in Appendix C - 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.
- Internationally recognized certification(s) for quality assurance and information security.

- 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.

The vendor selection criteria consist of 2 parts: Technical (accounting for 60% of the total score), based on submitted proposal and technical evaluation, and Price (accounting for 40% of the total score).

Proposal not passing the technical assessment will not be further considered.

The Price score is calculated based on the following formula:

Lowest price among qualified tenders / Offered price of the tenderer x 40%

15. Service Agreement Negotiation and Signature

The service agreement will be drawn up between the selected vendor and 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

Contacts	
Hong Kong Internet Registration Corporation Limited Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong +852 2319 2303 – telephone +852 2319 2626 – fax https://www.hkirc.hk *If you are not sure about the appropriate person to call, the receptionist can help you.*	**IT Project Manager** Ricky Fung +852 2319 3822 ricky.fung@hkirc.hk **Information Security Manager** Wilson YS Lam +852 2319 3849 ys.lam@hkirc.hk

Appendix A – Warranty

[start in next page]

To: Hong Kong Internet Registration Corporation Limited (HKIRC)

DearSir/Madam,

Warranty

(1) By submitting a tender, the Tenderer represents and warrants that in relation to the Request for Proposal of Recognized Certification Authority (RCA) and WebTrust Audit (Ref.: RFP-DCERT-RCA-WT-01):

(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 B – 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.: RFP-DCERT-RCA-WT-01
Title: Recognized Certification Authority (RCA) and WebTrust Audit

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 C – HKIRC Proposal Requirements

Proposal requirements	
Submission deadline	Please refer to Section 12 – Time Schedule, item no. 4 for the proposal submission deadline.
Hard copies	No Hard Copy is required
Electronic copy	Electronic copy is mandatory. It shall be sent by email to **ricky.fung@hkirc.hk** and **ys.lam@hkirc.hk**.
Proposal format	Specified in this document
Page count	40 pages or fewer
Font	Electronically published or typed. Times New Roman 12-point font.

1 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
- Audit Approach and Methodology
- Project management methodology
- Understanding of our requirements
- Knowledge and Advice on Projects/Services
- Deliverable and Services level
- Proposed Cost of Services and Payment Schedule
- Implementation Timetable
- Commercial and Payment Terms. e.g. Compensation for delay

2 Cover Page

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

Cover Page		
Project Title		
		Recognized Certification Authority (RCA) and WebTrust Audit (Tender Ref.: RFP-DCERT-RCA-WT-01)
Project Manager	Name:	
	Title:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
Company	Contact person:	
	Title:	
	Company name:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
	Website:	

3 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

4 Conflict of Interest Declaration

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

5 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. Please indicate where the key members station, i.e. local or non-local.

6 Audit Approach and Methodology

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

7 Project Management Methodology

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

8 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 with the requirements listed in the scope of service section; and briefly explain how they are achieved.

9 Knowledge and Advices on Projects/Services

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

project/service or projects/services with similar nature.

10 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.

11 Proposed Costs of Service and Payment Schedule

The vendor should provide the costs of RCA audit and WebTrust audit separately; and provide the breakdown of the cost of the whole project/service for each audit. The cost shall be broken down by milestone/phases. The payment shall be scheduled based on the milestones and/or deliverables.

For WebTrust audit, the item of "WebTrust Seal Application" should be quoted separately and the payment will be valid when this task is applicable, i.e. it is ready for WebTrust Seal application.

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 hours, non-working hours 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. (for at least the subsequent 3 years)
- Other direct costs including services, materials, supplies, postage, traveling, pocket money, etc.

12 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.

13 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.

Appendix D – HKIRC Information Security Policy: An Extract Relevant to Outsourcing

This document provides an extract of the HKIRC Information Security Policy (the "Policy") with the purposes of (a) introducing various measures and controls to be executed by HKIRC 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 applies to HKIRC'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 of the contractor and of any other subcontractors under the contractor's purview.

Herein, HKIRC would also set the expectation of any potential contractors that upon their indication of interest to the project, they shall be required in the subsequent stages to sign off a non-disclosure agreement ("NDA") on all information to be provided.

<-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><->

7. HUMAN RESOURCES SECURITY

7.1 PRIOR TO EMPLOYMENT

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.

7.1.1 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.

7.1.2 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.

7.1.3 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.

7.2 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.

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

7.2.2 All employees of the Organization and, where relevant, contractors and third-party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

7.3 TERMINATION AND CHANGE OF EMPLOYMENT

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

7.3.2 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.

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

14. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

14.2.7 The organization shall supervise and monitor the activity of outsourced system development.

16. INFORMATION SECURITY INCIDENT MANAGEMENT

16.1 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS

Security objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.3 Employees and contractors using the Organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.