# Digital Certificate Project

# Call for Tender

## (Tender Ref.: CFT-DCERT-01)

Version 1.0
Date: 21 February 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 ....1
1. Definitions ....3
2. About HKIRC ....4
3. Background of the Project ....5
4. The Required Services and System Functionalities ....9
4.1. Part A - Establishment of Certification Authority (CA) Infrastructure ....10
4.2. Part B - Integration with Domain Name Registration System (DNRS) ....17
4.3. Part C - Technical Support for Recognized Certification Authority (RCA) Application ....17
4.4. Part D – Certification Authority (CA) Operation ....18
4.5. Part E – Technical Support for Recognition by Common Web Browsers ....19
4.6. Part F - System Implementation, Project Management and Documentation (Core) 21
4.7. Part G - Information Security and Data Privacy Protection (Core) ....24
4.8. Part H - System Maintenance and Support (Core) ....29
4.9. Part I – Service Availability and Service Level (Core) ....31
4.10. Part J – Service Capacity and Sizing ....37
5. Limitation of Liability and Indemnity ....38
5.1. Service Level Agreement (SLA), Penalty, Service Credits and Contract Termination 38
5.2. Project Management Methodology and Review Meeting ....39
5.3. Intellectual Property Rights ....39
5.4. Software Source Code Escrow ....39
5.5. Sub-contracting/ Outsourcing ....40
6. Information Security ....40
7. Project Acceptance ....40
8. Anti-collusion ....41
9. Offering Advantages ....42
10. Ethical Commitment ....42
10.1. Prevention of bribery ....42
10.2. Declaration of Interest ....43
10.3. Handling of confidential information ....43
10.4. Declaration of ethical commitment ....44
11. Time Schedule ....44
12. Payment Schedule ....45
13. Elements of a Strong Tender ....45
14. Service Agreement Negotiation and Signature ....46
15. HKIRC Contacts ....46

Appendix A – Warranty ..... 47
Appendix B – Declaration Form by Contractor on their compliance with the ethical commitment requirements ..... 50
Appendix C – HKIRC Proposal Requirements ..... 52
1 Proposal Content ..... 53
2 Cover Page ..... 54
3 Executive Summary ..... 55
4 Conflict of Interest Declaration ..... 55
5 Company Background ..... 55
6 Methodology ..... 55
7 Project Management Methodology ..... 55
8 Understanding of our requirements ..... 55
9 Knowledge and Advices on Projects/Services ..... 55
10 Deliverable and Services level ..... 56
11 Implementation Time Table ..... 56
12 Commercial and Payment Terms ..... 56
13 Innovative Suggestions ..... 56
14 Proposed Costs of Service and Payment Schedule ..... 56
Appendix D – HKIRC Information Security Policy: An Extract Relevant to Outsourcing ..... 62
Appendix E - CA System Network Architecture ..... 64
Appendix F – HKIRC CA Websites ..... 68
Appendix G – Miscellaneous Support Functions ..... 69

# Summary

Hong Kong Internet Registration Corporation Limited (HKIRC) is going to commission a Service Provider ("the Contractor") to establish 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"

The Service Provider 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]; and support HKIRC in applying for being an RCA in the technical aspect. For offering SSL certificates to our customers, the CA System has to be fully integrated with our Domain Name Registration System (DNRS). The Service Provider will also provide subsequent system maintenance and support services.

Furthermore, Service Providers are encouraged to provide one-stop service for the Project by

[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

offering subsequent CA operation, including but not limited to issuing Certificate, verification of subscriber's identity, and providing technical advice and support for application for common web browsers' recognition.

The scope of services and system functionalities is detailed in Section 4 of this document.

The CA infrastructure has to be established by December 2025, i.e. within 6 months, and RCA has to be attained by April 2026, i.e. within 4 months.

Parties interested in providing this service shall submit **Expression of Interest (EOI) by 26th February 2024**. For those who have submitted EOI, they should **submit proposal** (see Appendix C) to the Group **no later than 5:30pm on 12th March 2025 (Hong Kong time)**.

Service Provider should submit Tender Proposal by email to HKIRC contacts (refer to Appendix C - HKIRC Proposal Requirements, electronic copy). Service Provider 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.

“DNRS” means the Domain Name Registration System of HKIRC and HKDNR.

“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 establishment of CA Infrastructure, and other services (i.e. CA operation) according to the requirements stipulated in Section 4 of this document.

“CFT” means this Call for Tender

“Tenderer” 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 http://www.hkirc.hk .

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

# 3. Background of the Project

a. Recognized Certification Authority (RCA)

HKIRC would like to serve as a Recognized Certification Authority (RCA) under ETO, COP and CPS. For the details of RCA, please refer to the website of Digital Policy Office (DPO) (Recognition of Certification Authorities and Certificates | Digital Policy Office). The CA Infrastructure built by the Service Provider must comply with the requirements of RCA. During the application for being recognized as RCA, the Service Provider also need to provide technical support to make the application successful.

In this Project, we target to issue the following recognized certificates, which are also listed in the website of DPO (Types of Digital Certificates | Digital Certificates for Electronic Transactions | Digital Policy Office):

| 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 (Note 1) | 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 (Note 1) | To conduct secure message transmissions by means of encryption/decryption |
| **Server** | Single or Multiple Servers / Web sites of Organisations (Note 1) | To verify the identity of web site(s) to the client browser and communicate in Secure Socket Layer (SSL) messages |
| **Governmental** | Staff of Government bureaux/departments (Note 2) | 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 (Note 1 and 2) | 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 organisations used for the applications as designated by their organisations |
| **Bank** | Personal / Corporate / Bank | To create digital signature on e-Cheque |
| **"iAM Smart"** | Hong Kong residents (Note 3) | 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") |

*Note 1: Organisations include Government bureaux/departments, non-Government organisations, universities/schools, private companies, etc.*

*Note 2: Offer of this type of recognized digital certificates requires prior arrangement between the recognized CA and the subscriber organisation.*

*Note 3: There are two versions of "iAM Smart", namely "iAM Smart" and "iAM Smart+". iAM Smart-Certs are designated for the subscribers who are holders of "iAM Smart+" account to conduct digital signing with legal backing under the Electronic Transactions Ordinance. Hong Kong residents should apply for "iAM Smart+" through designated self-registration kiosk, registration service counter or mobile registration team.*

b. Recognized by Common Web Browsers

To make the SSL certificates issued by our CA be applicable in the Internet, the SSL certificates must be recognized by common web browsers, including but not limited to:

i. Mozilla Firefox
ii. Google Chrome
iii. Microsoft Edge
iv. Apple Safari
v. Huawei HarmonyOS 華為 鴻蒙

To attain such recognition, Root Inclusion applications have to be submitted to web browsers to join their Trusted Root Certification Programs. As this process of completing the Programs of all the common web browsers would take time, this task will be incorporated in the scope of CA operation. The Service Provider has to provide technical advice and support to HKIRC, including but not limited to perform fine-tuning and enhancement in the CA Infrastructure and operation, for joining the Trusted Root Certification Programs successfully.

c. Project Timeframe

HKIRC targets to complete building the CA Infrastructure in which the Certificates can be issued successfully and properly by November 2025, i.e. within 6 months. Subsequently, HKIRC will submit application to DPO for being recognized as RCA, and we target to complete this process by April 2026, i.e. within 4 months.

The Service Provider has to complete its development of the CA Infrastructure with passing functional test by the target date (i.e. November 2025) in order to meet the above schedule. Passing RCA is also be one of the acceptance criteria and the Service Provider has to fully support HKIRC to make the RCA application successful.

d. CA Infrastructure

The Service Provider has to establish the CA Infrastructure, including but not limited to:

- CA System for Certificate issuance
- Web application for certificate subscription by customer; and verification of subscriber's identity and certificate issuance by operator
- Server infrastructure: hardware, software and/or Cloud services
- Secure facilities, i.e. data centre hosting

e. Integration with Domain Name Registration System (DNRS)

SSL certificates issued by the CA will be offered to our customer via our DNRS, where the issuance of SSL certificates (i.e. generating key pair) will be handled by the CA System. To provide one-stop service to our customers, a customer can purchase SSL certificate, generate certificate (key pair), and installation in our DNRS. Thus, the CA System has to be closely integrated with the DNRS for providing good customer experience.

f. CA Operation

Service Providers are encouraged to provide one-stop service by offering CA operation. The Service Provider has to carry out the work of issuing Certificates to subscribers, verifying certificate subscriber's identity and delivering Certificates through media. As mentioned, applying for common web browsers' trust and recognition is also part of the CA operation.

# 4. The Required Services and System Functionalities

The Solution proposed by the Service Provider must include proposals for performing operation and maintenance of the System and Services in accordance with ETO, COP and CPS(s) including:

1. Issuing, revoking or suspending and publishing all types of recognized certificates as / to be specified in the CPS(s).
2. Provision of the on-line publicly accessible Repository as specified in the CPS(s) for the publication of Certificates, CA Certificates, CRL(s) and other related information, which includes maintaining an archive of accepted certificates in the on-line repository.
3. Maintaining or handling of certificates and related system and paper records.
4. Provision of a web portal for the public to access to the HKIRC CA services and information.
5. Managing Registration Authority and other organisation(s) carrying out certain HKIRC CA functions and providing certain HKIRC CA services as requested by HKIRC during the Contract Period and ensuring the services provided by Registration Authority and the organisation(s) comply with ETO, COP and CPSs;
6. Ensuring provision of any new CA services or changes to CA services requested by HKIRC to comply with COP, ETO and any relevant laws of Hong Kong or to meet the public key infrastructure (PKI) standards and the CA developments decided by HKIRC;
7. Provision of services to all existing Certificate Subscribers and to ensure HKIRC to fulfil the obligations stipulated in any CPS and Certificate Subscriber Agreements with existing Certificate Subscribers.
8. Any other services provided to the public in accordance with the CPS(s).
9. Maintaining and modifying the PKI of HKIRC CA in providing CA services, including but not limited to:
    a. renewal of the root certificate(s) and subordinate certificates in due course; and

implementation or enhancement of System and Services to cope with PKI technology development and market demand. Examples of PKI technology development or market demand may include the use of Chinese domain name, stronger cryptographic algorithm and longer key length.

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:-

- **Part A** – establishment of certification authority (CA) infrastructure
- **Part B** – integration with Domain Name Registration System (DNRS)
- **Part C** – technical support for Recognized Certification Authority (RCA) application
- **Part D** – certification authority (CA) operation
- **Part E** – technical support for recognition by common web browsers
- **Part F** – system implementation, project management and documentation
- **Part G** – information security and data privacy protection
- **Part H** – system maintenance and support
- **Part I** – service availability and service level
- **Part J** – service capacity and sizing

The requirements are classified as Core and Optional items. Tenderers are advised to propose their solutions and services to cover both Core and Optional requirements to make their solutions be more comprehensive and complete. All Tenderers' proposed solutions and services must cover the Core requirements. For Optional items, Tenderers must provide quotation breakdown for each item in their proposals for our consideration. HKIRC reserves the right to accept partial or the whole proposal(s) submitted by Tenderer(s).

As the Project is evolving, HKIRC reserves the right to update the tender specifications and terms if and when necessary; and shall notify all the tenderers promptly.

## *4.1. Part A - Establishment of Certification Authority (CA) Infrastructure*

**Core Requirements:**

1. The Service Provider has to establish the Certification Authority (CA) infrastructure, including hardware, software, server infrastructure (Cloud and/or on-premises), secure facilities (i.e. data centre hosting) for the Certification Authority (CA) System.
2. The established CA Infrastructure is capable to issue, revoke or suspend, and publish all types of Certificates, including but not limited to:
   2.1. Personal
   2.2. Organizational
   2.3. Encipherment
   2.4. Server (including Domain Validation (DV), Organization Validation (OV) and Extended Validation (EV) certificates)
   2.5. Governmental

2.6. Organizational Role
2.7. Bank
2.8. “iAM Smart”
2.9. Digital Corporate Identity platform “CorpID”

3. The certificates includes but not limited to the following 3 validation types:
   3.1. Organization Validation (OV) - verifies the identity of the organization (e.g. a business, nonprofit, or government organization) of the Subject listed in the certificate, along with the location where the organization operates.
   3.2. Extended Validation (EV) - like OV, verifies the identity of an organization. However, EV represents a higher standard of trust than OV and requires more rigorous validation checks to confirm that the organization is properly registered with the authorities in its jurisdiction and that it meets the requirements set by the CA/Browser Forum.
   3.3. Domain Validation (DV) - lowest level of validation, and verifies that whoever requests the certificate controls the domain that the certificate protects.
4. The CA Infrastructure has to comply with all the requirements of RCA and common web browsers. Please refer to **Part C - Technical Support for Recognized Certification Authority (RCA) Application** and **Part E – Technical Support for Recognition by Common Web Browsers** for the details.
5. The HKIRC CA system should be operated using x86 and/or ARM based operating systems. Firewalls, routers and switches with appropriate access controls are implemented to segregate the servers into different network segments for better security control and protection. The data network should be TCP/IP based network.
6. The HKIRC CA system should be a multi-tiers application system running web servers, application servers, database servers, CA servers, reporting servers, directory servers, repeaters and responders for Online Certificate Status Protocol (OCSP), mail servers, file server and other software applications as appropriate for the operations of the HKIRC CA system.
7. Custom-made applications should be implemented to provide internal online application functions, background services, batch jobs, reports, external interfaces, online web applications accessible by the public, etc., for the Certificate services.
8. The HKIRC CA should maintain a web site that facilitates as a web portal for the public to access to the Certificate services and information. Online web application functions are implemented to facilitate the public easy access to the Certificate services.
9. The CA System, especially the online application and web portal, has to support most common client-side systems/ web browsers in the market.
10. Documentation has to be provided for the detailed system architecture design at both the application-level and infrastructure-level.
11. The CA should consist of the functions/ components including but not limited to:
    11.1. Certificate Profiles

11.2. Internal Online Application Functions
11.3. Background Application Functions
11.4. Reports
11.5. Online Internet Web Application Functions
11.6. Straight Through Processing (STP) program
11.7. CA System Infrastructure
11.8. Workstations
11.9. HKIRC CA Web Sites
11.10. System and Data Backup
11.11. Disaster Recovery (DR) Systems
11.12. Development and Testing Systems
11.13. Miscellaneous Support Functions

12. Internal online application functions provide interfaces for staff to operate the CA System and to provide Certificate services. The following sections describe the major internal online application functions:
    12.1. Login access control
    12.2. Certificates (all types) new application
    12.3. Certificates (all types) renewal
    12.4. Certificate subscription period extension
    12.5. Payment processing
    12.6. Certificate (all types) distribution, except TLS Certificates
    12.7. TLS Certificates are distributed through online web application
    12.8. Issuance of PIN mailer
    12.9. Certificate (all types except TLS Certificates) suspension and un-suspension
    12.10. Certificate (all types) revocation
    12.11. Certificate related information support
    12.12. Notification support
    12.13. FAQ (Frequently Asked Questions) function
13. Background application functions and services should be run by the system at scheduled time to provide supporting services. The following sections describe the major background application functions.
    13.1. Key-pairs generation
    13.2. Certificate Generation Agent
    13.3. Certificate Revocation Agent
    13.4. Certificate Posting Agent
    13.5. Notification service
    13.6. Certificate Revocation Lists (CRL) generation and publishing
    13.7. Audit trailing and logging
    13.8. Routine tasks and procedures

14. Reports are grouped into the following types:
    14.1. Reports for PIN mailer and Certificate storage medium delivery
    14.2. Service outlet collection summary and details reports
    14.3. Refund details reports
    14.4. Payment receipt reprinting report
    14.5. Certificates ready for renewal reports
    14.6. Business registration and certificate of incorporation / certificate of registration checking reports
    14.7. Certificates information reports
    14.8. Certificate generation and loading status reports
    14.9. Suspension / Un-suspension / Revocation reports
    14.10. Daily, weekly, monthly and yearly statistics on data and traffic reports
    14.11. Audit trail reports
    14.12. Letter mail generation reports
    14.13. Ad-hoc reports are created and generated on needed basis
15. Online Internet web-based application functions should provide a channel for the public and the subscribers to access to the Certificate services available through the Internet. The following sections describe the major online Internet web application functions.
    15.1. Certificate (Personal) new application
    15.2. Certificate (Personal) renewal
    15.3. Certificate (Personal) subscription period extension
    15.4. Online submission of TLS Certificate Signing Request (CSR)
    15.5. Certificate (Organisational) / Certificate (Encipherment) data confirmation
    15.6. Certificates (all types except Certificate (Server)) suspension
    15.7. Search and download Certificates (all types) from Repository
    15.8. Update Personal Information for Certificate (Personal) subscribers
    15.9. Download previously generated full Certificate Revocation List (CRL)
16. Straight Through Processing (STP) program is a system interface to receive certificate requests from various parties and pass to application server of the CA server for processing and issuance of Certificate (except TLS Certificate) in programmatic way.
17. Subscribers can make payment by payment methods via payment gateways, including but not limited to:
    17.1. Credit card (VISA, Master Card)
    17.2. Alipay (HK)
    17.3. Alipay (China)
    17.4. WeChat Pay
    17.5. PPS
    17.6. PayMe
    17.7. FPS

17.8. Bank-in slip (with proof uploaded to the System)

18. The CA System has to support multiple payment gateways, including but not limited to the followings, with auto failover in case the primary payment gateway is unavailable:
    18.1. Bank of East Asia (JETCO)
    18.2. AsiaPay
    18.3. PayPal
    18.4. GlobalPay
    18.5. QFPay
19. The CA System has to be integrated with the Financial Management System of HKIRC, via interface file and/or financial report.
20. The Service Provider should reference the system network architecture stated below for proposing its solution after doing a fair assessment. For the details, please refer to Appendix E - CA System Network Architecture.

| |
|---|
| Internet Segments (connected to Internet)<br>• Web Application Firewall (WAF)<br>• Load Balancer<br>• Firewall<br>• Internet Routers |
| DMZ Segments<br>• Directory Servers<br>• External Web Servers<br>• Mail Servers<br>• OCSP Servers<br>• Time Servers<br>• WSUS Server<br>• Load Balancers |
| CA Systems Internal Segments<br>• Application Servers<br>• Database Servers<br>• Internal Web Servers<br>• OCSP Servers<br>• Online CA Servers<br>• Domain Controllers<br>• System Management Servers<br>• Time Servers |

| |
|---|
| Offline CA Segment<br>• Offline CA Server |

21. To support reliable CA services, the following technologies/ components have to be considered in the design of CA Infrastructure:
    21.1. Server Virtualization Technology (VT), Containerization and Orchestration with High Availability (HA) to enhance server availability by mitigating the impact of hardware failures.
    21.2. Server and Application Monitoring (SAM) to facilitate round-the-clock server availability and application performance monitoring.
    21.3. Data Protection and Management (DPM) solution to securely back up valuable data and ensure data availability in the event of a disaster.
22. Furthermore, the CA Infrastructure has to include but not limited to the following security measures:
    22.1. Privileged Access Management (PAM) with Multi-Factor Authentication (MFA) to manage and control privileged access in a secure manner.
    22.2. Anti-Malware, EDR/ XDR, WAF, SIEM, IPS, together with MSS, to establish a defence-in-depth strategy against cybersecurity threats.
23. The HKIRC CA home web site should be managed for but not limited to:
    (Please refer to Appendix F – HKIRC CA Websites for more details)
    23.1. functioning as the web portal linking to HKIRC CA web pages or relevant web sites;
    23.2. publishing HKIRC CA services and other relevant information;
    23.3. posting CPS(s), root CA Certificate and subordinate CA Certificates;
    23.4. hosting online HKIRC CA web application functions;
    23.5. hosting of previously generated full CRL(s) for public download;
    23.6. publishing information and utilities to facilitate the use of Certificate by subscribers.
24. Miscellaneous Support Functions – please refer to Appendix G – Miscellaneous Support Functions for the details.
25. For verification of subscriber's identity, other than the traditional way, i.e. through face-to-face interaction. The Service Provider has to propose an alternative of conducting all the verification of subscriber's identity through online platform for our consideration.
26. The CA Infrastructure could be built on on-premises, Cloud or hybrid architecture. Service Providers please do fair assessment and propose their recommended approach, with full details (including all incurred relevant costs) and justification, for our consideration.
27. For secure facilities, all physical hardware included in the Project should be hosted in a data centre with tier level at least TIA-942 Tier 3+, ensuring compliance with the standard, covering aspects including but not limited to:
    27.1. Reliable power supply
        27.1.1. Dual feed PDU (Power Distribution Unit) on each rack.
        27.1.2. Redundant UPS (Uninterruptible Power Supply).
        27.1.3. Generator backup with sufficient fuel tanks.

27.2. Reliable air conditioning

27.2.1. Redundant CRAC (Computer Room Air Conditioning) units.

27.2.2. Redundant chiller plants.

27.2.3. Generator backup.

27.2.4. Raised-floor system with hot aisles and cold aisles design.

27.2.5. Water leakage detection system.

27.3. Fire protection and suppression

27.3.1. Fire alarm system.

27.3.2. FM-200 or NOVEC 1230 fire suppression system.

27.4. Security (24x7x365)

27.4.1. CCTV surveillance monitoring and recording.

27.4.2. Security guard patrol.

27.4.3. Physical security access control.

27.4.4. Pre-registration to access.

27.4.5. Security Operations Centre (SOC).

27.4.6. Network Operating Centre (NOC).

27.5. Connectivity

27.5.1. Dual lead-in.

27.5.2. Path diversity.

28. ITAI ready - the proposed solution must be ready to support ITAI[4] technologies (including but not limited to operating system, database, security, digital certification, etc.) in the design of the CA Infrastructure. Service Providers have to do fair assessment to determine the technologies to be adopted for the Project, but even if some of the components are not ITAI based at the initial stage of the Project, the design of the CA Infrastructure is still be able to cater for ITAI technologies and the CA Infrastructure is always ready to switch to an ITAI-based solution, without significant impact, at any time when necessary.

29. Verification of subscriber's identity through online platform:

29.1. iAM Smart – instead of conducting face-to-face verification of Certificate Subscriber's identity, iAM Smart can be applied to verify the identity of a person during the application process of Certificate.

29.2. CorpID – instead of checking application form with company chop manually, CorpID can be applied to verify the identity of an organization during the application process of Certificate.

[4] ITAI - Information Technology Application Innovation (信息技術應用創新 - 信創)

## *4.2. Part B - Integration with Domain Name Registration System (DNRS)*

**Core Requirements:**

30. SSL Certificate (for server) will be offered to our customers via our Domain Name Registration System, but the issuance of Certificate will be handled by the Service Provider.
31. HKDNR has been doing domain registration through a system namely Domain Name Registration System (DNRS). Other than offering domain names, it also offers SSL certificates to our customers.
32. The DNRS will adopt a Domain Registrar platform namely WHMCS. The SSL certificates have to be offered to our customers in the DNRS via WHMCS. For providing quality customer experience, the DNRS has to automate the SSL certificate ordering process by generating a Certificate Signing Request (CSR), submitting it to our certificate authority.
33. Automatic Certificate Management Environment (ACME) has to be supported for automating interactions between the certificate authority and our users' servers, allowing the automated deployment of public key infrastructure at very low cost.
34. Currently, HKID and Business Registration (BR) documents will be collected when registering Individual type and Organization type Domains respectively. For verification of identity, the proposed solution should leverage our current operation and streamline the process of Certificate application, i.e. not requiring the applicant to submit HKID/ BR documents again.

## *4.3. Part C - Technical Support for Recognized Certification Authority (RCA) Application*

**Core Requirements:**

35. HKIRC shall submit application to Certification Authority Recognition Office (CARO), Digital Policy Office (DPO) for recognition as a Recognized Certification Authority (RCA). For the details, please refer to the website: Application for Recognition | Digital Policy Office.
36. The Service Provider has to provide technical support, including providing technical information, fine-tuning and enhancement on the CA Infrastructure for complying with the RCA requirements, including but not limited to:
    36.1. Provisions of the Electronic Transactions Ordinance (Cap. 553) (ETO)
    36.2. The Code of Practice for RCA. Please refer to Code of Practice for Recognized Certification Authorities| Digital Policy Office for the details
    36.3. Certificate Policy for Mutual Recognition of Electronic Signature Certificates issued by Hong Kong and Guangdong. Please refer to Certificate Policy for the MR scheme.

## *4.4. Part D – Certification Authority (CA) Operation*

**Optional Requirements:**

37. The Service Provider has to take all reasonable care in issuing Certificates to the Certificate Applicants or Certificate Subscribers and has to take all reasonable care to persons who may rely upon these Certificates (including without limitation to maintain CPS up to date, and make the Repository available for public access in accordance with the CPS).
    37.1. Certification Practice Statement – The Service Provider has to publish for public knowledge and maintain up to date CPS(s) for the types, classes or descriptions of Certificates issued.
    37.2. Trusted System – The Service Provider has to use a Trusted System in performing its services, including the generation and management of the Key Pairs, the generation and management of subscribers' Key Pairs if appropriate, the issuance, renewal, suspension or revocation of Certificates, the giving of notice of the issuance, renewal or revocation of Certificates, the provision of the Repository, and the publication of Certificates and other information in the Repository.
    37.3. Certificates and Recognized Certificates – The Service Provider has to ensure the separate private keys are used to sign recognized certificates and certificates which are not recognized certificates respectively. The Service Provider has to ensure that recognized certificates
    37.4. Verification of Subscriber's Identity – The Service Provider has to specify in the relevant CPS that corresponds to a particular type, class or description of recognized certificates the procedure to very the identity of a person who applies for such a recognized certificate. The Service Provider has to retain copies of the documentary evidence that identifies the subscribers.
    37.5. Repository - the Service Provider has to make available at least one on-line and publicly accessible Repository for the publication of recognized certificates and related information. It shall ensure that the Repository or Repositories are implemented through Trusted Systems and conform to the service levels in respect of the operation of the Repository or Repositories specified in the CPS(s).
    37.6. Disclosure of Information - The Contractor shall publish in the Repository or Repositories:
        37.6.1. the CA Certificates that contain the public key corresponding to the private key used to digitally sign Certificates;
        37.6.2. the suspension, revocation or non-renewal notice of the CA Certificates; and

37.6.3. any other fact that materially and adversely affects either the reliability of a recognized certificate issued or the ability of the Contractor and/or HKIRC to perform its services under the ETO.

37.6.4. Assessment of Compliance with the ETO and COP – submission of report on yearly basis for the compliance with the provisions of the ETO and the COP as are specified under the COP.

37.6.5. Declaration of Compliance with the ETO and COP – a statutory declaration for compliance with the provisions of the ETO and COP as are specified under the COP.

37.6.6. Adoption of Standards and Technology – the Service Provider shall continuously review and, where appropriate, improve and update the standards and technology of the System and Services.

37.6.7. Inter-operability - to reduce barriers for digital signatures supported by recognized certificates to be widely accepted, the Service Provider has to, wherever applicable, adopt an open and common interface to facilitate the verification by others of digital signatures supported by the Certificates.

37.6.8. For verification of subscriber's identity, other than the traditional way, i.e. through face-to-face interaction. The Service Provider should also support an alternative of conducting all the verification of subscriber's identity through online platform, if applicable.

38. The Service Provider has to store the generated Certificates (i.e. key pair) into a media (e.g. USB flash drivers or hardware tokens) and deliver it to the subscribers securely.
39. Service Providers have to detail their plan of delivering their CA Operation, including the arrangement of operation centre for the CA Operation, for our consideration.

## *4.5. Part E – Technical Support for Recognition by Common Web Browsers*

**Optional Requirements:**

40. HKIRC shall submit Root Inclusion applications to common web browser vendors, including but not limited to the followings, to join their Trusted Root Certification Programs:
    - 40.1. Mozilla Firefox
    - 40.2. Google Chrome
    - 40.3. Microsoft Edge
    - 40.4. Apple Safari
    - 40.5. Huawei HarmonyOS 華為 鴻蒙

41. The Service Provider has to provide technical support and advice for joining the Trusted Root Certification Programs.
42. The Service Provider has to make the CA Infrastructure and operation comply with the requirements of common web browsers, including but not limited to:
    - 42.1. WebTrust for CA program (please refer to Principles and criteria and practitioner guidance - CPA Canada), which covers:
        - 42.1.1. Webtrust for CA
        - 42.1.2. Webtrust for CA – Extended Validation SSL
        - 42.1.3. Webtrust for CA – SSL Baseline
        - 42.1.4. Webtrust for CA – Network Security
    - 42.2. CA/Browser Forum baseline requirements, including:
        - 42.2.1. Baseline Requirements for TLS server certificates (please refer to Baseline Requirements for TLS Server Certificates | CA/Browser Forum)
        - 42.2.2. Extended Validation Guidelines for TLS server certificates (please refer to EV Guidelines for TLS Server Certificates | CA/Browser Forum)
        - 42.2.3. Network and Certificate System Security requirements (please refer to Network and Certificate System Security Requirements | CA/Browser Forum)
    - 42.3. - Common Web Browser Root Program policies, including:
        - 42.3.1. Mozilla Root Store Policy (please refer to Mozilla Root Store Policy — Mozilla)
        - 42.3.2. Microsoft Trusted Root Program requirements (please refer to Program Requirements - Microsoft Trusted Root Program | Microsoft Learn)
        - 42.3.3. Google Chrome Root Program Policy (please refer to Chrome Root Program Policy, Version 1.5)
        - 42.3.4. Apple Root Certificate Program (please refer to Root Certificate Program - Apple)
    - 42.4. The Adobe Approved Trust List (AATL) technical requirements, version 2.0 (please refer to Adobe Approved Trust List)
43. The Service Provider has to propose qualified auditor(s) for the audits related to common web browsers' recognition, which would be recruited by HKIRC directly.

## *4.6. Part F - System Implementation, Project Management and Documentation (Core)*

The Contractor shall carry out system implementation works, with proper documentation, and perform project management to ensure the Project is delivered within the planned project schedule and with acceptable quality and information security level:

| # | Project Activities/ Deliverables | Documentation (by the Contractor) |
|---|---|---|
| 1. | Project management<br>• Project review meetings (at least once per month)<br>• Ad-hoc project review meetings | • Project Implementation Plan (by phases, by timeline)<br>• Cut-Over and Go-Live Plan<br>• Change Management Plan<br>• Post-Go-Live Support Plan<br>• All Meeting Agendas<br>• Meeting Minutes<br>• Weekly and/or Monthly project progress reports |
| 2. | Project Initiation | • Project initiation document (PID)<br>• Project Chapters |
| 3. | System Analysis and Design | • User requirement specification:<br>o Business Requirements (BRD)<br>o Functional Requirements (FRD)<br>o Non-business/ System Requirements (SRS)<br>o Requirement Traceability Matrix (RTM)<br>o Database and Storage Requirements<br>o Product Functions for UI/ UX<br>• Gap analysis report:<br>o Comparing the new system capabilities with user requirements<br>o Identify the gap and develop business cases<br>o Recommendations and Resolution to the gap<br>• Mock-up/ prototype<br>• Functional specifications:<br>o Functional Data Flow Diagram (DFD)<br>o Use Case Diagrams<br>o User Interface<br>o Performance<br>o Manageability / Maintainability<br>o System Interface / Integration<br>o Security |

| # | Project Activities/ Deliverables | Documentation (by the Contractor) |
|---|---|---|
| | | • Technical specifications:<br>  ○ System Architecture Diagram (SAD)<br>  ○ System Design Diagram (SDD)<br>  ○ Network Architecture Diagram (NAD)<br>  ○ RDBMS Database Design<br>  ○ Database Schema and Entity Relationship Diagram (ERD)<br>  ○ Database Data Dictionary<br>  ○ User Account Management<br>  ○ Password Management<br>  ○ Security Related Setup<br>  ○ System Interface and Connections<br>  ○ Integration with 3rd Parties Software and System |
| 4. | Server Infrastructure Setup | • Network Diagram<br>• System and Network Configuration |
| 5. | Application Development | • Change Request:<br>  ○ Change Request Documentation (CR) |
| 6. | Testing | • Test Plan, Test Scenarios |
| 6.1. | Quality assurance (by the Contractor) | • Quality Assurance Report |
| 6.2. | System integration testing | • Test Cases, Test Scenarios<br>  ○ Cover all the functions for the CA System<br>  ○ For each test case, clear description of how to conduct the test (with step-by-step instructions and screenshots), expected results, etc. have to be provided<br>• Test Report<br>  ○ Report all the identified issues, status, and remedial actions for outstanding issues |
| 6.3. | User acceptance testing | • Test Cases, Test Scenarios<br>  ○ Cover all the functions for the CA System<br>  ○ For each test case, clear description of how to conduct the test (with step-by-step instructions and screenshots), expected results, etc. have to be provided<br>• Test Report |

| # | Project Activities/ Deliverables | Documentation (by the Contractor) |
|---|---|---|
| | | ○ Report all the identified issues, status, and remedial actions for outstanding issues |
| 7. | Training | |
| 7.1. | User training<br>• For Operator and IT Department | • Training Plan and Schedule<br>• User manual<br>○ Full workflow with step-by-step instructions, screenshots (and/or video clips) has to be provided<br>○ By Word<br>• User training presentation materials (e.g. by PowerPoint, Word)<br>• User training recordings |
| 7.2. | System administration training<br>• For IT Department | • System administration manual (for CA System and Infrastructure)<br>○ Full workflow with step-by-step instructions, screenshots (and/or video clips) has to be provided<br>○ By Word |
| 7.3. | Operator training<br>• For Operator | • Certification Authority (CA) Operation Manual<br>○ Workflow of issuing, revoking, suspending, publishing Certificate<br>○ Workflow of verification of Certificate subscriber's identity<br>○ Workflow of delivering Certificate to subscriber<br>○ Full workflow with step-by-step instructions, screenshots (and/or video clips) has to be provided<br>○ Service level monitoring |
| 8. | Disaster recovery drill | • Disaster recovery plan and procedures |
| 9. | Business Continuity Planning | • Business continuity plan (BCP) |
| 10. | Security Risk Assessment and Audit<br>• The exercise will be conducted by a third-party service provider; and the vulnerabilities will be fixed by the Contractor | • SRAA report(s) [by a third-party service provider] |

| # | Project Activities/ Deliverables | Documentation (by the Contractor) |
|---|---|---|
| 11. | Privacy Impact Assessment (PIA)<br>• The exercise will be conducted by a third-party service provider; and the remedial actions will be implemented by the Contractor | • PIA report(s) [by a third-party service provider] |
| 12. | Recognized Certification Authority, WebTrust, Extended Validation (EV) and other CA-related Audit(s) | • Audit report(s) [by third-party service provider(s)] |
| 13. | System nursing | After new system goes on Production (go live), system nursing period must be provided at least 6 months to support the entire system functions. |

## *4.7. Part G - Information Security and Data Privacy Protection (Core)*

Information security and data privacy are crucial to safeguard the digital assets of/ derived from the System. Security risk assessment and audit (SRAA), Red Team's penetration testing and Privacy impact assessment (PIA) will be conducted by a third-party service provider at different stages of the Project. The Contractor must collaborate with the security service provider for carrying out those exercises, and fix the identified vulnerabilities/ issues accordingly.

| # | Requirements |
|---|---|
| 1. | Security by design |
| 1.1. | The approach of "security by design" has to be adopted throughout the entire system development life cycle. SRAA and PIA professionals would be involved in the system implementation works, i.e. starting from system analysis and design.<br><br>The personal data protection must be compliant with the following prevailing regulatory requirements and/or ordinance including HK Cap. 486 Personal Data (Privacy) Ordinance; and must reference China's Personal Information Protection Law (PIPL) and EU General Data Protection Regulation (GDPR). |
| 2. | Security risk assessment and audit (SRAA) (by a third-party service provider) |
| 2.1. | A third-party security service provider will be recruited by HKIRC for the project. There will be at least 1 time of SRAA conducted for the CA Infrastructure:<br>• After user acceptance testing (i.e. pre-production)<br><br>Additional SRAA exercise(s) might be required if there are significant concerns or |

| # | Requirements |
|---|---|
| | findings raised in the previous exercise(s). |
| 2.2. | Code scanning shall be conducted and the Contractor has to provide source code for this exercise. |
| 3. | Red Team's penetration testing (by a third-party service provider) |
| 3.1. | A third-party security service provider will be recruited by HKIRC for the project. There will be at least 1 time of penetration testing (in either grey or white box approach) conducted for the CA Infrastructure:<br>• After user acceptance testing (i.e. pre-production) |
| 4. | Privacy impact assessment (PIA) (by a third-party service provider) |
| 4.1. | A third-party security service provider will be recruited by HKIRC for the project. There will be at least 1 time of PIA conducted for the CA Infrastructure:<br>• After user acceptance testing (i.e. pre-production)<br><br>Additional PIA exercise(s) might be required if there are significant concerns or findings raised in the previous exercise(s). |
| 5. | Vulnerability fixing and system enhancement for data privacy |
| 5.1. | The Contractor must fix the vulnerabilities and data privacy issues identified/ raised in the SRAA, penetration testing and PIA according to the testing results and reports. |

The Contractor also needs to observe and comply with the following security guidelines, if and when applicable, when designing its solution; and during the system implementation and on-going system maintenance:

1. Security for Recognized Certification Authority (RCA)
   1.1. IT Security Guidelines (G3) of Digital Policy Office (DPO)
   1.2. Baseline IT Security Policy (S17) of DPO
   1.3. Security measures to be covered in this Project include but not limited to:
      1.3.1. Tiered firewall with network segmentation should be implemented to separate external and internal networks.
      1.3.2. Intrusion Prevention System (IPS) and log analytics should be implemented to detect and block malicious traffic.
      1.3.3. Endpoint Detection and Response (EDR) should be implemented to detect and provide effective response to potential security activities.
      1.3.4. Privileged Access Management (PAM) with Multi-Factor Authentication (MFA) should be implemented to manage and control privileged access.
      1.3.5. Local and off-site backups should be implemented to provide fast backup and provide additional layer of protection against backup copies being compromised by cyberattacks.

1.3.6. Data-at-rest and Data-in-transit encryption should be implemented to protect against unauthorized access to physical storage devices and interception over the network.

1.3.7. Sufficient resilience should be implemented to prevent disruption of the essential services provisioned.

1.3.8. Quarterly vulnerability scanning should be adopted to ensure risks and vulnerabilities are well mitigated and compliance with regulatory standard is maintained.

2. Website and Web Application Security

2.1. Common Threats for Websites and Web Applications

2.1.1. Ensure no components with known vulnerability.

2.1.2. Ensure System/security with proper configuration.

2.1.3. Ensure defence in depth concept in design.

2.1.4. Ensure enough control to prevent from Distributed Denial of Service (DDoS) attack.

2.1.5. Ensure enough control to defense Altering website code and/or web defacement.

2.1.6. Ensure enough control to prevent from Web forgery.

2.2. Additional Threats for Web Applications

2.2.1. Ensure enough control to minimize the web application security risks mentioned in OWASP Top 10 and other good practices.

3. Website and Web Application Life Cycle

3.1. Project Initiation

3.1.1. Ensure project requirements such as functions and features of new website/web application, which are operation or business focused.

3.1.2. Ensure proper data classification involved to the website and web application.

3.1.3. Ensure enough security requirements for the new project such as encryption requirements, data storage protection and physical protection requirement are mentioned in the project documentation.

3.2. Feasibility Study

3.2.1. Ensure security requirement analysis and security planning if the project is technically feasible.

3.3. Systems Analysis & Design

3.3.1. Ensure security requirements based on the business needs, including the legal and regulatory requirements (e.g. the Personal Data (Privacy) Ordinance) and the best practice security requirements.

3.3.2. Ensure corresponding security controls should be incorporated to the design such that secure architecture, design and structure can be achieved.

3.3.3. Ensure appropriate technical and organisational security measures should be adopted to protect personal data from unauthorised or accidental access, processing, erasure or other use, including but not limited to ensuring the compliance with all applicable laws and regulations, conducting privacy impact assessment to identify and manage data protection risks, ensuring the processes and systems are designed such that the collection and processing of personal data are limited to what is necessary for the identified purpose, and improving staff awareness of the possible consequences (such as violation of security policies, damage of government image, disciplinary actions) when personal data is breached.

3.3.4. Ensure adequate security review conducted in the design stage in the SDLC, which serves as a checkpoint to ensure necessary security requirements are identified and incorporated in the system design.

3.4. Implementation

3.4.1. Ensure the requirements defined and the suggested counter measures from risk for the assessment result should be followed for system/application development.

3.4.2. Ensure that the website or web application is ready for production with acceptable risks for security assurance.

3.4.3. Ensure inspection and acceptance of developed components for website and web application and integration of security controls should be performed to current environment, or new production environment, if any.

3.4.4. Ensure the web application secure coding practices in developing web applications should be observed so as to withstand some common web application security vulnerabilities.

3.4.5. Ensure source Code Review and Protection.

3.4.6. Ensure security risk assessment should be performed before the production launch of the website or web application.

3.4.7. Ensure privacy impact assessment should be conducted to examine the adequacy, effectiveness and practicability of the planned protection measures for the protection of personal data.

3.5. Post-Implementation

3.5.1. Ensure a post-implementation review should be performed such that there is no unexpected problem during the system installation and deployment task.

3.5.2. Ensure all proposed changes or patches should be verified in testing environment and they do not incur security issue to the production environment.

3.5.3. Ensure backup task should be performed to prevent from unexpected loss of information and to ensure that fallback is available when the change is failed.

3.5.4. Ensure security monitoring should be adopted to detect malicious activities targeted to website and web application.

3.5.5. Ensure an incident response and handling procedure should be defined for website and web application.

3.5.6. Security risk assessments for websites and web applications should be performed at least once every two years or after major changes.

3.6. Decommission

3.6.1. Ensure that the replacement is run properly and necessary migration has been performed such as data and user migration in case there is a replacement of website or web application for the original system.

4. Security Consideration for Web Content Management System and Web 2.0

4.1. Web Content Management System (WCMS)

4.1.1. Ensure WCMS is subject to the same security threats and operation process vulnerabilities as other web applications.

4.2. Web 2.0

4.2.1. Ensure Security Concerns and Precautionary Measures should be adopted in the use of Web 2.0 technologies.

5. Security Guidelines and Standards:

5.1. ISO27001

5.2. EU General Data Protection Regulation (GDPR) (need to reference this regulation and do fair assessment)

5.3. China's Personal Information Protection Law (PIPL) (need to reference this regulation and do fair assessment)

5.4. Payment Card Industry (PCI) Security Standards

5.5. OWASP Top 10, OWASP Code Review Guide (Please refer to OWASP_Code_Review_Guide_v2.pdf)

5.6. CIS Microsoft Windows Server 2022 Benchmark (Please refer to CIS_Microsoft_Windows_Server_2022_Benchmark_v3.0.0.pdf)

## *4.8. Part H - System Maintenance and Support (Core)*

| # | Requirements |
|---|---|
| 1. | Unlimited e-mail and telephone/ virtual conference support |
| 1.1. | Support operating hours:<br>• 7 days x 24 hours |
| 2. | System bug fixing |
| 2.1. | The Contractor has to conduct an assessment and effort estimation for every reported issue (i.e. system bug) and perform bug fixing according to the plan. |
| 3. | System patching and vulnerability fixing |
| 3.1. | System patching and vulnerability fixing have to conducted by the Contractor, including but not limited to regular System hotfix, Operating System (OS) patching, database patching, critical vulnerability fixing, according to the importance of the identified vulnerabilities and business impact incurred by the patch(s). |
| 4. | Disaster recovery (DR) drill |
| 4.1. | DR drill will be run once per year, and the Contractor has to provide support in this exercise at the application level. |
| 5. | Incident response, system recovery and critical issue fixing |
| 5.1. | For any critical issue (top severity), system down and security breach, 24x7 support has to be provided for resuming the System into the normal state as soonest as possible. |
| 6. | Supporting regular security scanning and audit |
| 7. | HKIRC reserves the rights to do ad-hoc system enhancement or develop add-on components based on the Contractors' solution without voiding the warranty. |

**1. <u>Problem classification</u>**

| Severity | Definition |
|---|---|
| Critical (Severity 1) | Production server or other mission critical system(s) are down and no workaround is immediately available.<br>• All or a substantial portion of our mission critical data is at a significant risk of loss or corruption.<br>• Have had a substantial loss of service.<br>• Business operations have been completely halted.<br>• Payment gateways have been completely not functioning |
| Major (Severity 2) | Major functionality is severely impaired.<br>• Operations can continue in a restricted fashion, although long-term productivity might be adversely affected. |

| Severity | Definition |
|---|---|
| | • A major milestone is at risk. Ongoing and incremental installations are affected.<br>• A temporary workaround is available. |
| Minor (Severity 3) | Partial, non-critical loss of functionality of the software.<br>• Impaired operations of some components, but allows the user to continue using the software.<br>• Initial installation milestones are at minimal risk. |
| Cosmetic (Severity 4) | General usage questions.<br>• Cosmetic issues, including errors in the documentation |

## 2. Security classification

| Severity | Definition |
|---|---|
| Critical (Severity 1) | Intruders can easily gain control of the host, which can lead to the compromise of the entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors. |
| Major (Severity 2) | Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, and unauthorized use of application and unauthorized use of data. |
| Medium (Severity 3) | Intruders may be able to determine the operating system running on the host and view banner version. |
| Minor (Severity 4) | Intruders can collect information about the host (open ports, services, etc.) |

**3. Problem resolution/ vulnerability fixing time**

a. Core CA functions, including but not limited to the following. The list of functions are subject to the final negotiation for this Agreement:
   i. Issuing, revoking or suspending, publishing Certificates, especially those are issued online with automation
   ii. Provision of the online publicly accessible Repository for the publication of Certificates, CA Certificates, Certificate Revocation Lists (CRL)
   iii. Integration with DNRS, iAM Smart, CorpID, and other external systems through APIs or protocols
   iv. Customer-facing web application for subscribing Certificate, verification of subscriber's identity, etc.

| Severity | Response time | Resolution/ fixing time |
|---|---|---|
| **1** | 30 minutes | 4 hours |
| **2** | 2 hours | 12 hours |
| **3** | 4 hours | 60 hours |
| **4** | 8 hours | 120 hours |

b. Non-core function, such as:
   i. Back-end system for the operation team
   ii. Back-end functions, such as financial management, transaction enquiry

| Severity | Response time | Resolution/ fixing time |
|---|---|---|
| **1** | 30 minutes | 8 hours |
| **2** | 2 hours | 24 hours |
| **3** | 4 hours | 120 hours |
| **4** | 8 hours | 240 hours |

## *4.9. Part I – Service Availability and Service Level (Core)*

**1. System and Services Availability**

The Service Provider has to meet the Availability Level of the System and Services (for Core CA functions, listed below) of at least 99.99% (Availability Level).

Core CA functions, including but not limited to:

a. Issuing, revoking or suspending, publishing Certificates, especially those are issued online with automation
b. Provision of the online publicly accessible Repository for the publication of Certificates, CA Certificates, Certificate Revocation Lists (CRL)
c. Integration with DNRS, iAM Smart, CorpID, and other external systems through APIs or protocols
d. Customer-facing web application for subscribing Certificate, verification of subscriber's identity, etc.

The Availability Level is a measure of the length of time of the System and Services required to be made available in accordance with the CPS(s) and the service levels as specified in this Tender Document. Availability is the proportion of the measurement period (one month) that the System and Services are available.

The Availability Level is expressed as a percentage by using the following formula:

$$\frac{\text{(Scheduled Uptime – Total duration of Outage(s) \# during Scheduled Uptime)}}{\text{Scheduled Uptime}} \times 100\%$$

# The CA Infrastructure has to adopt multiple sites with Active-Active resilience; and local Active-Active resilience, i.e. minimum 4 nodes. If the cluster has more than half of the nodes is down (for example, 3 out of 4 nodes are down), it will be treated as "Outage".

Scheduled Uptime is defined as the time that the System and Services are scheduled to be available in accordance with the Service Levels excluding periods of unavailability due to Force Majeure.

Outage is defined as an event where the System or Services becomes unavailable. Each outage shall be counted on an incremental basis, regardless of whether the same problem recurs several times over a measurement period. If multiple users experience the same problem simultaneously, this is counted as only one outage.

## 2. Services Availability/ Level Requirements:

| Services | Service Availability | Service Level |
|---|---|---|
| Help Desk Support (for Customer) | • 7 x 24 help desk support is required<br>• Provide help desk support services via multiple channels. | • At least 90% of incoming requests are handled by various channels proposed. For telephone call, within 12 seconds and 3 ringing tone.<br>• At least 60% of incoming calls will be answered by live operators within 12 seconds or 3 ringing tone within the proposed operating hours. |
| Application processing | • Complete processing the Certificate applications according to the published performance pledges of HKIRC. | • e-Cert (Personal) - 3 days<br>• e-Cert (Organisational) - 10 days<br>• e-Cert (Encipherment) - 10 days<br>• e-Cert (Server) - 10 days |
| On-line Repository | • Make the Repository available for public access on a substantially 24 hours per day, 7 days per week basis, subject to scheduled maintenance and any emergency maintenance | • At least 99.99% Availability Level |

| Services | Service Availability | Service Level |
|---|---|---|
| Technical Support (for HKIRC) | • 7 x 24 technical support for maintaining the Service Level Agreement (SLA) | • Please refer to **3. Problem resolution/ vulnerability fixing time** of **4.8. Part H - System Maintenance and Support** |
| System problem/ failure determination and resolution | • The System has to be "always on". 7 x 24 service for system problem/ failure determination and resolution is required for maintaining the SLA. | • Please refer to **3. Problem resolution/ vulnerability fixing time** of **4.8. Part H - System Maintenance and Support** |
| Performance and capacity management | • Perform capacity planning annually or when necessary. | • Please refer to **Part J – Service Capacity and Sizing**<br>• The System capacity must be able to accommodate the demand (i.e. within ±10% deviation) within 12 months after annual planning<br>• 99.99% Available Level for Core CA functions |

| Services | Service Availability | Service Level |
|---|---|---|
| Load Balancing and Resilience | • Multiple sites with Active-Active resilience are required. Load balancing has to be implemented to ensure the performance and minimize the downtime.<br>• In case of one of the Active-Active sites is down, i.e. the infrastructure is degraded, it has to be resumed promptly in order to meet the pledged system/ service availability.<br>• A Disaster Recovery (DR) system has to be established as the last resort. | • At least 99.99% Availability Level |
| Disaster Recovery (DR) and/or business continuity plan and drill | • Review DR/business continuity plan and risk management plan and conduct DR drill at least once in every 12 months.<br>• Ensure the success of DR in every drill exercise and perform remedial action accordingly, if needed. | • Review and planning have to be completed without outstanding issue within 2 months |
| Management reports to HKIRC | • Provide HKIRC with management reports at 1-month intervals. | • Each management report, with acceptable quality, shall be delivered to HKIRC within 5 working days after the last day of the month the management report covers. |

| Services | Service Availability | Service Level |
|---|---|---|
| Requests from HKIRC, including enhancement, enquiries and reports | | • For general requests which can be handled within 5 man-days, deliver the required enhancement, enquiry result or report within 3 working days upon request.<br>• For other requests requiring more efforts, an implementation plan has to be given on the next working day upon request. |
| Services relating to iAM Smart-Cert | • Services relating to iAM Smart-Cert is available on a substantially 24 hours per day, 7 days per week basis, subject to scheduled maintenance and any emergency maintenance | • At least 99.99% Availability Level |
| Services relating to CorpID-Cert | • Services relating to CorpID-Cert is available on a substantially 24 hours per day, 7 days per week basis, subject to scheduled maintenance and any emergency maintenance | • At least 99.99% Availability Level |

## *4.10. Part J – Service Capacity and Sizing*

### 1. CA Infrastructure Capacity (Core)

The CA Infrastructure is required to have sufficient capacity to accommodate the following demand and growth. The CA Infrastructure has to be scalable to allow the infrastructure to scale out for the growth of demand over time:

| | **Number of Certificates per Year** |
|---|---|
| Year 1 | ~15,000 |
| Year 2 | ~15,750 |
| Year 3 | ~16,538 |
| Year 4 | ~17,365 |
| Year 5 | ~18,233 |

The CA Infrastructure can also be scaled out to accommodate the demand of ~2,000,000+ Certificates per Year ultimately:

| **Certificate Application Type** | **Max. Number of Certificates per Year** |
|---|---|
| Issued/ renewed with manual processes | ~300,000 |
| Issued/ renewed automatically | ~1,800,000 |

### 2. CA Operation (Optional)

The CA Operation is required to have sufficient capacity to accommodate the following demand and growth. The CA Operation has to be scalable to allow the operation team to scale out for the growth of demand over time:

| | **Number of Certificates per Year** |
|---|---|
| Year 1 | ~15,000 |
| Year 2 | ~15,750 |
| Year 3 | ~16,538 |
| Year 4 | ~17,365 |
| Year 5 | ~18,233 |

The CA Operation can also be scaled out to accommodate the demand of ~2,000,000+ Certificates per Year ultimately:

| Certificate Application Type | Max. Number of Certificates per Year |
|---|---|
| Issued/ renewed with manual processes | ~300,000 |
| Issued/ renewed automatically | ~1,800,000 |

# 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), Penalty, 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, stated below, or any applicable remedial actions (at the Service Provider's own cost) for compensation for the service which did not meet the SLA.

Monthly review on Service Provider's performance as per the SLA will be conducted. As the Service Credit scheme, if the Service Provider fails to meet the SLA of a particular item for 2 consecutive months (i.e. in 2 consecutive performance reviews), the Service Provider has to compensate HKIRC in terms of 5 man-days of professional services for HKIRC's use in this Project.

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.

The Project Manager assigned by the Service Provider for this Project must possess the qualification(s) of PMP and/or PRINCE2 and/or other equivalent qualification, with at least 10-year solid project management experience in the IT field.

## *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.

### *5.5. Sub-contracting/ Outsourcing*

Any agreement resulting from this procurement exercise will specifically be with the Contractor, and will require the performance of the service to be provided by the agreed experts of the Contractor as specified in the tender response. Any further sub-contracting and/or out-sourcing of work shall require HKIRC's express approval. Sub-contracting and/or out-sourcing do/does not exempt the Contractor from their obligations and they remain liable and accountable for subcontractor actions.

# 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. System analysis and design (SA&D)
   All the SA&D documents are endorsed. The system design can fulfill the tender specification, user requirements and business needs for the Digital Certification service.

2. User acceptance testing / security assessment and audit (SRAA) / privacy impact assessment
   All identified vulnerabilities, at all levels of severity, have to be fixed.

3. Data migration (if applicable), system integration and system live run
   The CA Infrastructure and System are fully functional and operational for the Digital Certification service. The design and functionality of the CA Infrastructure must comply with RCA and common web browsers' requirements.

4. Recognized Certification Authority (RCA) attained
   Recognized by DPO as a Recognized Certification Authority (RCA) for all the recognized Certificates included in this Project.

5. System nursing and warranty
   No outstanding post-Production system issue and operational issue by the end of the system nursing and warranty period.

# 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. Ethical Commitment

## *10.1. 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.

## *10.2. 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).

## *10.3. 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.

### *10.4. 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.

## 11. Time Schedule

| | Tasks | To be Completed by | Remark |
|---|---|---|---|
| 1 | Publish CFT | 17-Feb-2025 | |
| 2 | Express of interest | 24-Feb-2025 | |
| 3 | Sign NDA with all interested vendors | 26-Feb-2025 | |
| 4 | Deadline for vendors to submit tender | 12-Mar-2025, 5:30pm | |
| 5 | Sign service agreement contract with the appointed vendor | 30-May-2025 | |
| 6 | Kick-start of the project | 2-Jun-2025 | |
| 7 | Certification Authority infrastructure completed | 30-Nov-2025 | |
| 8 | Application for Recognized Certification Authority (RCA) completed | 30-Apr-2026 | |
| 9 | Project completion (System Live Run, Ready for Operation) | 30-Jun-2026 | |

# 12. Payment Schedule

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

| Milestone | Items | Payment |
|---|---|---|
| 1. | System analysis and design (SA&D) | 5% |
| 2. | User acceptance testing / security assessment and audit / privacy impact assessment | 10% |
| 3. | Data migration, system integration and system live run | 20% |
| 4. | Recognized Certification Authority (RCA) attained | 35% |
| 5. | System nursing and warranty (6-month) | 30% |

# 13. 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 | 70% |
| Price | 30% |

The Price score is calculated based on the following formula:

*Lowest price among qualified tenders / Offered price of the tenderer x 30%*

# 14. 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.

# 15. HKIRC Contacts

HKIRC Contacts information

| ***Contacts*** | |
|---|---|
| **Hong Kong Internet Registration Corporation Limited**<br>Unit 501, Level 5,<br>Core C, Cyberport 3,<br>100 Cyberport Road,<br>Hong Kong<br><br>+852 2319 2303 - telephone<br>+852 2319 2626 - fax<br>http://www.hkirc.hk<br><br>*If you are not sure about the appropriate person to call, the receptionist can help you.* | **Primary Contact:**<br>**IT Project Manager**<br>Ricky Fung<br>+852 2319 3822<br>ricky.fung@hkirc.hk<br><br>**Secondary Contact:**<br>**Manager, IT Infrastructure**<br>Keith Chan<br>+852 2319 3845<br>keith.chan@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 tender of Digital Certificate Project (Ref.: CFT-DCERT-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.:
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 C – HKIRC Proposal Requirements

| ***Proposal requirements*** | |
|---|---|
| Submission deadline | Please refer to Section 11 – 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 cc **keith.chan@hkirc.hk** . |
| Proposal format | Specified in this document |
| Page count | Total 100 pages for Overall Proposal (including Technical Proposal and Price Proposal) |
| Font | Electronically published or typed. Times New Roman 12-point font. |

# *1 Proposal Content*

Please submit 2 proposals: Technical Proposal and Price Proposal separately, i.e. by 2 separate files/ documents.

The Technical 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 Advice on Projects/Services
- Deliverable and Services level
- Implementation Time Table
- Commercial and Payment Terms. e.g. Compensation for delay
- Innovative Suggestions

The Price Proposal should contain the following:

- Cover Page
- Proposed Cost of Services and Payment Schedule

## *2 Cover Page*

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

| ***Cover Page*** | | |
|---|---|---|
| Project Title | | |
| | | Digital Certificate Project<br>(Tender Ref.: CFT-DCERT-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 HKIRC/ HKDNR.

## *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.

## *6 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 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.

## *12 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.

## *13 Innovative Suggestions*

The vendor should propose innovative suggestions, such as pro-innovation and ESG proposals, which would bring benefits and values to the Project.

## *14 Proposed Costs of Service and Payment Schedule*

The vendor should provide the breakdown of the cost of the whole project/service, i.e. quotation and Bill of Materials (BOM). 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 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
- Other direct costs including services, materials, supplies, postage, traveling, pocket money, etc.

Please provide your quotation with the following summary:

| # | Item | Core/ Optional | Remarks |
|---|---|---|---|
| 1. | Establishment of certification authority (CA) infrastructure, including:<br>• Integration with DNRS<br>• Technical support for RCA application | | |
| 1.1. | Hardware | Core | 5-year warranty |
| 1.2. | Cloud Service | Core | For subscription based, please quote the fees for 4 years |
| 1.3. | Software | Core | For subscription based, please quote the fees for 4 years |
| 1.4. | Secure facilities | Core | For data centre hosting, please quote the fees for 4 years<br>For Cloud, please estimate the subscription cost based on the initial sizing, and quote the fees for 4 years |
| 1.5. | CA System (i.e. application) with project management and implementation services | Core | |
| 1.6. | Verification of subscriber's identity by iAM Smart | Core | |
| 1.7. | Verification of subscriber's identity by CorpID | Core | |
| 1.8. | ITAI alternative solution | Optional | Even if some of the system components are not based on ITAI technologies, Service Provider has to offer an ITAI alternative solution for consideration |
| 2. | System support and maintenance for CA infrastructure | Core | • Please quote the fees for 4 years, with yearly breakdown<br>• 2-year base + 2-year renewable contract<br>• 2-year base contract: no fee increment is allowed<br>• 2-year renewable contract: annual increment has to follow OR does not exceed the Consumer Price Index (Composite) of Hong Kong |

| # | Item | Core/ Optional | Remarks |
|---|---|---|---|
| 3. | Certification authority (CA) operation, including:<br>• Technical support for common web browsers' recognition | Optional | • Please quote the fees for 4 years, with yearly breakdown<br>• 2-year base + 2-year renewable contract<br>• 2-year base contract: no fee increment is allowed<br>• 2-year renewable contract: annual increment has to follow the Consumer Price Index (Composite) of Hong Kong<br>• Please detail the arrangement of operation centre for your services of CA operation |

Service Providers please fill in your price offer in the following table:

| | | | | Breakdown (HK$) | | | | |
|---|---|---|---|---|---|---|---|---|
| **#** | **Item** | **Core/ Optional** | **HK$** | **Year 1** | **Year 2** | **Year 3** | **Year 4** | **Remarks** |
| 1. | Establishment of certification authority (CA) infrastructure, including:<br>• Integration with DNRS<br>• Technical support for RCA application | **Sub-total:** | | | | | | |
| 1.1. | Hardware | Core | | | | | | One-off with 5-year warranty |
| 1.2. | Cloud Service | Core | | | | | | 4-year subscription |
| 1.3. | Software | Core | | | | | | Perpetual + 4-year warranty<br>OR<br>4-year subscription |
| 1.4. | Secure facilities | Core | | | | | | 4-year data centre rental<br>AND/OR<br>4-year Cloud subscription |
| 1.5. | CA System (i.e. application) with project management and implementation services | Core | | | | | | One-off |

| | | | | Breakdown (HK$) | | | | |
|---|---|---|---|---|---|---|---|---|
| # | Item | Core/ Optional | HK$ | Year 1 | Year 2 | Year 3 | Year 4 | Remarks |
| 1.6. | Verification of subscriber's identity by iAM Smart | Core | | [redacted] | | | | One-off |
| 1.7. | Verification of subscriber's identity by CorpID | Core | | | | | | One-off |
| 1.8. | ITAI alternative solution | Optional | | | | | | H/W:<br>one-off with 5-year warranty<br>S/W:<br>Perpetual + 4-year warranty<br>OR<br>4-year subscription |
| 2. | System support and maintenance for CA infrastructure | Core | | | | | | 4-year service<br>For the 3rd and 4th year, if following CPI for inflation, please indicate clearly in your quotation, and this factor can be determined in the future. |

| | | | | Breakdown (HK$) | | | | |
|---|---|---|---|---|---|---|---|---|
| **#** | **Item** | **Core/ Optional** | **HK$** | **Year 1** | **Year 2** | **Year 3** | **Year 4** | **Remarks** |
| 3. | Certification authority (CA) operation, including:<br>• Technical support for common web browsers' recognition | Optional | | | | | | 4-year service<br>• For the 3rd and 4th year, if following CPI for inflation, please indicate clearly in your quotation, and this factor can be determined in the future. |

# 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.

# Appendix E - CA System Network Architecture

| | |
|---|---|
| Directory Servers | Certificates, CRL(s), ARL (Authority Revocation List), root CA Certificates and subordinate CA Certificates are published in the directory servers. The directory servers should support LDAP protocol and adopt a hierarchical design to provide an effective directory services management. The directory servers should be configured in load balancing and redundant mode to provide better performance and availability services. |
| External Web Servers | The external web servers should support HTTP/HTTPS protocols, and provide the web interface for the public to access to various online web-based services and information. The external web servers should support multiple web domains by using virtual hosting feature. The external web servers should be configured in load balancing and redundant mode to provide better performance and availability services. |
| Mail Servers | The SMTP based mail servers should provide an e-mail gateway for issuing electronic mail notification to applicants/subscribers through the Internet. The mail servers should be configured in load balancing and redundant mode to provide better performance and availability services. |
| Application Servers | The application servers will run CA application services. The application servers should be configured in active-active cluster mode to provide better performance and availability services. |
| Internal Web Servers | The internal web servers should support HTTP/HTTPS protocols, and provide the interfaces for the access to various internal online applications. The internal web servers should be configured in redundant mode to provide better availability to internal online application. |
| Database Servers | 1. The database servers should be running on the operating system based cluster in active-standby mode (or preferably active-active mode) to provide resilience support for the database systems. The database servers should be accessible to the internal systems and services inside HKIRC CA internal network only with appropriate access controls.<br>2. The HKIRC CA system should maintain multiple (four) relational database systems (RDBMS) for its daily operations. The |

| | |
|---|---|
| | database systems store different data items for different operational and security needs.<br>3. One of the database systems should be the CA database repository maintained by the online CA servers. Except for database administration and maintenance functions, the CA database should be manipulated by the online CA servers directly. Apart from configuration data, data stored in the CA database includes, but not limited to :<br>a. Generated certificates;<br>b. Certificate profiles;<br>c. Certificate Revocation Lists (CRL(s));<br><br>4. The other (three) database systems should be manipulated by the CA application system. The data stored in these database systems include, but not limited to :<br>d. System configuration parameters;<br>e. Operating users access control data;<br>f. Application data;<br>g. Subscriber and subscription information;<br>h. Certificates information;<br>i. Payment records;<br>j. Notification information and records;<br>k. Audit trail records. |
| Online CA Servers | 1. The online CA servers should be the core systems to handle the day-to-day subscriber certificates generation, revocation operations (or suspension / un-suspension operations for future expansion), and to generate the CRL(s) at configured schedules.<br>2. The online CA servers should sign the generated certificates and CRL(s) using the respective subordinate CA keys. The private keys of the subordinate CA Certificates should be installed in Hardware Security Modules (HSM) that are connected to the online CA servers to provide the secure storage of the private keys.<br>3. Multiple online CA servers should be installed and configured in active-active mode to provide better performance and availability services. |
| Offline CA Server | 1. The offline CA server provides the services and management for the operations of the root CA. The private keys of the root CA must be loaded into a Hardware Security Module (HSM) for the secure storage of the root CA keys. An internal database should |

| | |
|---|---|
| | be maintained for its operations. The offline CA server should be a standalone system without network connection, and should be powered off when not in operations.<br>2. The offline CA server should be used to manage the CA Certificates and should used to generate the authority revocation lists ("ARL") as and when required or once every year. |
| Network and systems management | 1. Centralised network and systems management software should be installed to provide centralised support and management of the system components.<br>2. A network and systems monitoring server should be installed to perform host based monitoring by incorporating monitoring agents installed on the monitored servers. It should also support the SNMP protocols for monitoring the SNMP enabled devices. The management server should provide the monitoring of critical processes, system exceptions, network availability and system healthiness of the CA systems and send out alerts to the system administrators through pagers.<br>3. The backup management server should provide the centralised backup management of backup jobs on the different servers installed with backup management agents.<br>4. The anti-virus management console should provide a centralised management of the anti-virus software agent configuration, virus signature update, virus scanning schedules and virus alerts to the system administrators. |
| Time synchronisation | Time synchronisation among systems and network equipment should be based on NTP protocol. |
| Domain controllers | 1. Windows domain controllers should be implemented to control the security policies and provide user accounts management of the workstations so that only the required services and functions will be accessible by the authorised user accounts through the workstations.<br>2. The domain controllers should be configured in active-active mode to provide better performance and domain services availability. |
| File Server | The file server should provide file storage and retrieval services for filled application forms and generated reports. |
| Reporting server | The reporting server should provide reporting functions for generating reports based on pre-defined reporting templates. Generated reports should be exportable for further processing. |

| | |
|---|---|
| OCSP Repeaters and Responders | The responders should communicate with HKIRC CA System to determine the responses to OCSP requests and pass them to the repeaters. The repeaters act as the proxy of the responders to interface with the end clients to receive their request and to provide them the responses. |
| Workstations | 1. The workstations should be Windows based personal computers supporting Traditional Chinese user interfaces. The system configurations must be hardened for better security control and protection. Anti-virus software should be installed on all workstations to protect against possible virus attacks. Virus signatures should be updated regularly and automatically through anti-virus management console.<br>2. Workstations should be equipped with the necessary accessories, including but not limited to, smart card readers, receipt printers, bar code scanners, keypads, dual-display graphics card, dual LCD displays, printers, etc. |

# Appendix F – HKIRC CA Websites

1. The HKIRC CA home web site should be managed for but not limited to:
   a. functioning as the web portal linking to HKIRC CA web pages or relevant web sites;
   b. publishing HKIRC CA services and other relevant information;
   c. posting CPS(s), root CA Certificate and subordinate CA Certificates;
   d. hosting online HKIRC CA web application functions;
   e. hosting of previously generated full CRL(s) for public download;
   f. publishing information and utilities to facilitate the use of Certificate by subscribers.
2. Designated online service end-points / web sites should be used to host online HKIRC CA web application functions.
3. A designated web page should be used as the repository to publish the latest full CRL and if applicable the partitioned CRL(s).
4. All the above web sites may be hosted in the same web servers using virtual hosting services of the web server application.
5. The information posted in HKIRC CA web sites should be published in English, Traditional Chinese and Simplified Chinese.
6. TLS Certificates should be installed in the web sites of HKIRC CA to support SSL connections using HTTPS protocol as and when required.

# Appendix G – Miscellaneous Support Functions

1. Change PKCS#12 PIN utility
2. A utility for changing the PKCS#12 PIN of Certificate file (in PKCS#12 format) should be implemented and available for public download at the HKIRC CA web site. The utility should be available in English and Traditional Chinese versions.
3. Trial Certificate support to Relying Parties
4. In order to provide support for Relying Parties to test their Certificate based applications, the following trial Certificate supports should be provided:
    a. Trial certificates
    b. Trial CRL[5]
    c. Trial directory services
5. The trial systems should be maintained using the same systems and facilities of the development and testing systems.
6. The trial systems should also generate and publish the trial CRL(s) regularly. Trial directory server accessible through LDAP protocol should be also maintained to publish the trial certificates and the trial CRL(s). The trial CRL(s) and trial directory server should be available for access over the Internet. Relying Parties should be able to use these trial facilities to test their Certificate based applications.

[5] CRL - Certificate Revocation List