Digital Certificate Project

Call for Tender

(Tender Ref.: CFT-DCERT_PHASE2-01)

Version 1.0
Date: 11 Jun 2026

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 2
2. About HKIRC 5
3. Background of the Project 6
4. The Required Services and System Functionalities 10
4.1. Part A - Establishment of Certification Authority (CA) Infrastructure for iAM Smart 13
4.2. Part B - Technical Support for Recognized Certification Authority (RCA) Application and Maintenance 18
4.3. Part C – Certification Authority (CA) Operation for iAM Smart 18
4.4. Part D - System Implementation, Project Management and Documentation 22
4.5. Part E - Information Security and Data Privacy Protection 25
4.6. Part F - System Maintenance and Support 30
4.7. Part G – Service Availability and Service Level 32
4.8. Part H – Service Capacity and Sizing 37
5. Migration service for the existing CA operations for Personal Certificates, Organization certificates, Bank certificates to new CA Infrastructure (Optional) 38
6. Limitation of Liability and Indemnity 42
6.1. Service Level Agreement (SLA), Penalty, Service Credits and Contract Termination 42
6.2. Project Management Methodology and Review Meeting 43
6.3. Intellectual Property Rights 43
6.4. Software Source Code Escrow 43
6.5. Sub-contracting/ Outsourcing 44
7. Information Security 44
8. Project Acceptance 44
9. Anti-collusion 45
10. Offering Advantages 45
11. Ethical Commitment 46
11.1. Prevention of bribery 46
11.2. Declaration of Interest 46
11.3. Handling of confidential information 47
11.4. Declaration of ethical commitment 47
12. Time Schedule 48
13. Payment Schedule 49
14. Elements of a Strong Tender 49
15. Service Agreement Negotiation and Signature 51

16. HKIRC Contacts 51
Appendix A – Warranty 52
Appendix B – Declaration Form by Service Provider on their compliance with the ethical commitment requirements 55
Appendix C – HKIRC Proposal Requirements 57
1 Proposal Content 58
2 Cover Page 59
3 Executive Summary 60
4 Conflict of Interest Declaration 60
5 Company Background 60
6 Methodology 61
7 Project Management Methodology 61
8 Understanding of our requirements 61
9 Knowledge and Advices on Projects/Services 61
10 Deliverable and Services level 62
11 Implementation Time Table 62
12 Commercial and Payment Terms 62
13 Innovative Suggestions 62
14 Proposed Costs of Service and Payment Schedule 63
Appendix D – HKIRC Information Security Policy: An Extract Relevant to Outsourcing 69
Appendix E - CA System Network Architecture 71
Appendix F – Miscellaneous Support Functions 75
Appendix G – Hardware BOM 76

Summary

Hong Kong Internet Registration Corporation Limited (HKIRC) is one of Recognized Certification Authority (RCA) granted recognition to issue certificates, including Digital Certificate (Personal), Digital Certificate (Organisational), and Digital Certificate (Encipherment) under the name of Hong Kong Certification Authority (HKCA). This tender is going to commission a Service Provider to establish a dedicated certification authority (CA) infrastructure for integration with iAM Smart system.

The Service Provider will establish a new separate CA infrastructure with a view to supporting the digital certificate requirements of the iAM Smart system. The CA Infrastructure, covering hardware, software, server infrastructure and secure facilities, etc., must be compliant with ETO[1], COP[2] and CPS(s)[3]. The Service Provider will also provide subsequent system maintenance and support services as well as 24x7 operations of the CA Infrastructure.

Furthermore, Service Providers are encouraged to provide one-stop service for the Project by offering subsequent CA operation, including but not limited to digital certificate related operations, namely issuance, suspension, revocation and OCSP, verification of subscriber's identity, and providing technical advice regarding the smooth running of the CA Infrastructure as appropriate.

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

The CA Infrastructure has to be established by 1st February 2027, and acceptance of production implementation has to be attained by 1st April 2027. After successful hand-over and acceptance of the CA Infrastructure, the operation contact would last for 2 (mandatory) + 2 (optional) years, i.e. a maximum of 4 years in total.

Parties interested in providing this service shall **submit Tender Proposal** (see Appendix C) to

[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

the Group **no later than 23:59pm on 10th July 2026 (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 Service Provider" means 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" means the body issuing digital certificates, i.e. HKIRC.

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

"The Infrastructure", "CA Infrastructure" and "The System" means Certification Authority infrastructure in this Project. It consists of the CA System, server infrastructure and secure facilities.

"The Services" and "The Project" means 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

"RCA" means Recognized Certification Authority. In short, Recognized Certification Authority (RCA) is a certification authority formally approved by the Government under the Electronic

Transactions Ordinance (Cap. 553). An RCA acts as a trusted third party that issues digital certificates to verify the identity of individuals and organizations in electronic transactions.

Recognition is granted only to certification authorities that meet stringent government requirements on security, reliability, and operational standards, ensuring that their services are trustworthy and compliant.

Digital certificates issued by an RCA support legally recognized digital signatures, particularly for transactions involving government entities, and provide assurance of authenticity, integrity, and non-repudiation in electronic communications. Please refer to the follow link for the introduction of Recognized Certification Authorities in Hong Kong | ETO | Digital Policy Office and CA Recognition Scheme

"ETO" means Electronic Transactions Ordinance. In short, the Electronic Transactions Ordinance (ETO) of Hong Kong (Cap. 553) provides the legal framework governing electronic transactions. It establishes that electronic records and electronic signatures have the same legal status and enforceability as their paper-based and handwritten counterparts, subject to specified conditions.

The Ordinance also defines the use of digital signatures supported by recognized digital certificates for transactions involving government entities, and introduces a voluntary recognition scheme for Certification Authorities (CAs) to ensure trust, identity verification, and integrity in electronic transactions.

Overall, the ETO underpins the legal validity, security, and trustworthiness of electronic communications and digital certificate services in Hong Kong, forming a critical regulatory foundation for digital signature and certification authority operations. Please refer to the follow link for the original Ordinance View Electronic Transactions Ordinance (Cap. 553) and details Electronic Transactions Ordinance (Chapter 553) | Digital Policy Office.

"COP" means The Code of Practice. In short, it is for Recognized Certification Authorities, issued under the Electronic Transactions Ordinance (Cap. 553), defines the standards and procedures governing the operation of Recognized Certification Authorities (RCAs).

It sets out requirements on security controls, operational processes, and compliance practices to ensure that digital certificate services are reliable, secure, and trustworthy.

Compliance with the COP is mandatory for RCAs and forms a key basis for maintaining government recognition, thereby ensuring the integrity, authenticity, and legal reliability of digital signatures and electronic transactions. The following is the details of Code of Practice for Recognized Certification Authorities (Official)

"CPS" means Certification Practice Statement (CPS). In short, Certification Practice Statement (CPS) is a formal document published by an RCA that defines the detailed procedures, controls, and practices for issuing, managing, and revoking digital certificates.

It provides transparency on how the CA verifies identities, protects cryptographic keys, and ensures the security and integrity of its certificate services. The CPS enables relying parties to assess the trustworthiness of the CA and forms a critical basis for ensuring the authenticity, integrity, and legal reliability of digital signatures and electronic transactions. The iAM Smart related CPS is attached. HKCA and its service provider must follow the CPS to provide service.

"PKI" means Public Key Infrastructure (PKI), it is a framework of technologies, policies, and processes used to create, manage, and validate digital certificates and cryptographic keys for secure electronic communications. It enables trusted identity verification, data confidentiality, integrity, and non-repudiation in digital transactions.

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)
After being appointed as a Recognized Certification Authority, HKIRC would like to prepare for supporting the digital certificate related requirements of iAM Smart in compliance with ETO, COP and CPS. The CA Infrastructure built by the Service Provider must comply with the requirements of RCA.

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 current digital certificates that HKCA would (and plan to) issue are as follows:

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 Organization (Note 1)	To conduct secure message transmissions by means of encryption/decryption
Server	Single or Multiple Servers / Web sites of Organizations (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
Organizational 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

In this Project, we target to issue the following recognized certificates (iAM Smart) and provide a 7 x 24 support to DPO 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
"iAM Smart"	Hong Kong residents (Note 1)	To conduct digital signing via the "iAM Smart" system to handle statutory documents and procedures

Note 1: 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. Project Timeframe

HKIRC targets to complete building the CA Infrastructure in which the iAM Smart Certificates can be issued successfully and properly by 1st February, 2027, i.e. within 6 months. Subsequently, HKIRC will submit application to DPO for necessary change regarding the original RCA infrastructure, and we target to complete this process before production launch by 1st April 2027, i.e. within 8 months.

The Service Provider must complete its development of the CA Infrastructure and passing functional tests by the target date (i.e. 1st February, 2027) in order to meet the above schedule. Passing RCA Audit is also one of the acceptance criteria and the Service Provider has to fully support HKIRC to make the RCA application successful. The list of the hardware and network equipment are listed in the appendix G (Hardware BOM)

c. CA Infrastructure

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

- CA System for Certificate issuance
- API for certificate subscription by customer; and verification of subscriber's identity and certificate issuance by operator
- Server infrastructure: hardware, software, information security services and/or necessary management services. HKIRC would provide a list of hardware as System Infrastructure. With justifications acceptable to HKIRC, the Service Provider may suggest minimal upgrade or exchange of the provided infrastructure upon fully utilising the HKIRC provided System Infrastructure. (The detail of hardware list in Appendix G – Hardware BOM)
- Secure hosting facilities, i.e. data centre hosting

The relationship of the Concept and Functions:

Concept	Function
ETO	Legal framework
RCA	Government-approved CA
COP	RCA Operating rules that must be followed

d. CA Operation (iAM Smart)

Service Providers are encouraged to provide one-stop service by offering CA operation (iAM Smart). The Service Provider must carry out the work of issuing Certificates to subscribers, verifying certificate subscriber's identity. The detail requirements are listed in Section 4 "The Required Services and System Functionalities".

e. Migration of Existing CA infrastructure. (Optional)

Currently, HKCA already have CA infrastructure for supporting the Personal, Organizational, Encipherment, Server, Governmental, Organizational Role and Bank certificate. Service providers are also invited to provide the necessary service(s) to migrate the current infrastructure to the iAM Smart CA infrastructure. For detail information and requirements please refer to the Session 5.

4. The Required Services and System Functionalities

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

1. Operate the iAM Smart certificate service on behalf of HKIRC under HKIRC's governance, in full compliance with ETO, COP, applicable CPS(s) and all relevant Hong Kong regulatory requirements.
2. Perform full lifecycle management of recognized certificates, including issue, revoke, suspend, renew and publish, covering all certificate types defined in the CPS(s) designated by HKIRC, e.g. iAM Smart certificates for digital signing.
3. Conduct subscriber identity verification in accordance with CPS requirements, retain all supporting evidence, and support secure online verification where applicable.
4. Operate and maintain a trusted PKI system, including CA systems, HSM, key management, certificate processing, repository, logging and security controls.
5. The new iAM Smart CA system must incorporate a Hardware Security Module (HSM) and be at least fully ready to use the SM2 cryptographic algorithm. Service Provider are required to provide the detail specifications in Appendix C
6. The service provider shall be responsible for conducting the SRAA, PIA, and all required security audits. Furthermore, the Service Provide shall provide full support and necessary assistance for the HKIRC to perform RCA and other related audits.
7. Provide and maintain a public repository to publish certificates, CA certificates, CRLs and all required disclosures in accordance with CPS, COP and regulatory requirements.
8. Ensure all certificate-related records (electronic and paper) are complete, accurate and auditable.
9. Manage and oversee Registration Authorities (RA) and supporting entities, ensuring all CA-related activities comply with ETO, COP and CPS(s).
10. Deliver and support CA services (iAM Smart), including new services, enhancements, and changes required by HKIRC, in line with PKI standards, CPS(s) and regulatory requirements.
11. Maintain and enhance the HKIRC CA PKI infrastructure, including certificate lifecycle management (e.g. root / subordinate renewal) and upgrades aligned with technology evolution and cryptographic standards.
12. Support interoperability and open standards, enabling broad verification and acceptance of digital signatures.
13. Securely manage certificate generation, storage and delivery, including handling of key materials and activation where applicable.

14. Maintain up-to-date operational procedures and CPS-aligned controls, and support HKIRC in compliance reporting, audits, regulatory submissions and remediation for ongoing RCA compliance.
15. Ensure security, availability, resilience, backup, disaster recovery, and incident response, meeting requirements for recognized CA operations and Critical Infrastructure operations.
16. Support HKIRC in infrastructure changes, regulatory submissions and technical implementation, including providing necessary documentation.
17. Support HKIRC in infrastructure changes, regulatory submissions and technical implementation up to Critical Infrastructure Ordinance (Cap. 653) requirements (Code Of Practices) , including providing necessary documentation.
18. Operate as an accountable outsourced service provider under HKIRC's governance, including oversight, approval and audit rights.
19. Continuously improve systems and services to meet PKI technology developments and market demands, such as adoption of stronger cryptographic algorithms and longer key lengths.

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

(Core)

- **Part A** – establishment of certification authority (CA) infrastructure for iAM Smart
- **Part B** – technical support for Recognized Certification Authority (RCA) application and maintenance.
- **Part C** – certification authority (CA) operation for iAM Smart
- **Part D** – system implementation, project management and documentation
- **Part E** – information security and data privacy protection
- **Part F** – system maintenance and support
- **Part G** – service availability and service level
- **Part H** – service capacity and sizing

The tenderers are advised to propose their solutions and services to cover all requirements to make their solutions more comprehensive and complete. All Tenderers' proposed solutions and services must cover all the requirements with quotation breakdown for each item in their proposals for 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 for iAM Smart

Core Requirements:

1. The Service Provider has to establish the Certification Authority (CA) infrastructure, including hardware, software, server infrastructure, secure facilities for the Certification Authority (CA) System regarding iAM Smart.
   1.1. The established CA Infrastructure is capable to issue, revoke or suspend, and publish all types of Certificates, including but not limited to: "iAM Smart"
2. The CA Infrastructure has to comply with all the requirements of RCA. Please refer to **Part B - Technical Support for Recognized Certification Authority (RCA) for application and maintenance** for the details.
3. The new iAM Smart CA system should be connected with DPO (iAM Smart system) through API. (DPO will provide further API info upon contract award)
4. 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.
5. The CA system in this Project should be a multi-tiers application system running front end 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 CA system in this Project.
6. Custom-made applications should be implemented to provide internal online application functions, background services, batch jobs, reports, external interfaces, API applications accessible by the public, etc., for the Certificate services.
7. The HKIRC CA shall maintain the website (hkca.hk) Types of Digital Certificate – Hong Kong Certification Authority (HKCA), as a public web portal for access to certificate service information. The CA System, in particular the web portal, supports the most commonly used client operating systems and web browsers in the market. The Service Provider shall provide relevant information for updating of the hkca.hk website upon request of HKIRC.
8. Documentation has to be provided for the detailed system architecture design at both the application-level and infrastructure-level.
9. The CA System in this Project should consist of the functions/ components including but not limited to:
   9.1. Certificate Profiles
   9.2. Reports
   9.3. Online Internet API Functions
   9.4. CA System Infrastructure
   9.5. Workstations

9.6. System and Data Backup
9.7. Disaster Recovery (DR) Systems
9.8. Development and Testing Systems
9.9. Miscellaneous Support Functions

10. The Service Provider shall be responsible for internal online application functions that provide interfaces for staff to operate the CA System (iAM Smart) and to provide Certificate services. The following sections describe the major internal online application functions:
    10.1. Login access control
    10.2. Certificates (iAM Smart) new application
    10.3. Certificates (iAM Smart) renewal
    10.4. Certificate subscription period extension
    10.5. Certificate (iAM Smart) distribution
    10.6. Issuance of PIN mailer
    10.7. Certificate suspension and un-suspension
    10.8. Certificate (iAM SMART) revocation
    10.9. Certificate related information support
    10.10. Notification support
    10.11. FAQ (Frequently Asked Questions) function
11. 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.
    11.1. Key-pairs generation
    11.2. Certificate Generation Agent
    11.3. Certificate Revocation Agent
    11.4. Certificate Posting Agent
    11.5. Notification service
    11.6. Certificate Revocation Lists (CRL) generation and publishing
    11.7. Audit trailing and logging
    11.8. Routine tasks and procedures
12. Reports are grouped into the following types:
    12.1. Reports for PIN mailer and Certificate storage medium delivery
    12.2. Service outlet collection summary and details reports
    12.3. Refund details reports
    12.4. Payment receipt reprinting report
    12.5. Certificates ready for renewal reports
    12.6. Business registration and certificate of incorporation / certificate of registration checking reports
    12.7. Certificates information reports
    12.8. Certificate generation and loading status reports

12.9. Suspension / Un-suspension / Revocation reports

12.10. Daily, weekly, monthly and yearly statistics on data and traffic reports

12.11. Audit trail reports

12.12. Letter mail generation reports

12.13. Ad-hoc reports are created and generated on needed basis

13. Online API functions should provide a channel for the DPO iAM Smart team to access to the Certificate services available through the specific channel. The following sections describe the major online API functions.

13.1. Online submission of Certificate Signing Request (CSR)

13.2. Certificate (iAM Smart) data confirmation

13.3. Certificates (IAM Smart) suspension

13.4. Search and download Certificates (iAM Smart) from Repository

13.5. Update Personal Information for Certificate (iAM Smart) subscribers

13.6. Download previously generated full Certificate Revocation List (CRL)

14. 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.

15. 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) • Web Application Firewall (WAF) • Load Balancer • Firewall • Internet Routers
DMZ Segments • Directory Servers • External Web Servers • Mail Servers • OCSP Servers • Time Servers • WSUS Server • Load Balancers
CA System Internal Segments • Application Servers • Database Servers • Internal Web Servers

- OCSP Servers
- Online CA Servers
- Domain Controllers
- System Management Servers
- Time Servers

Offline CA Segment

- Offline CA Server

16. To support reliable CA services, the following technologies/ components have to be considered in the design of CA Infrastructure:
    16.1. Server Virtualization Technology (VT), Containerization and Orchestration with High Availability (HA) to enhance server availability by mitigating the impact of hardware failures.
    16.2. Server and Application Monitoring (SAM) to facilitate round-the-clock server availability and application performance monitoring.
    16.3. Data Protection and Management (DPM) solution to securely back up valuable data and ensure data availability in the event of a disaster.
17. Furthermore, the CA Infrastructure has to include but not limited to the following security measures:
    17.1. In order to manage and control privileged access in a secure manner. The Privileged Access Management (PAM) with Multi-Factor Authentication (MFA) is recommended. Service provider can also provide alternative security solution with detail specification.
    17.2. Anti-Malware, EDR/ XDR, WAF, SIEM, IPS, together with MSS, to establish a defense-in-depth strategy against cybersecurity threats.
18. Miscellaneous Support Functions – please refer to Appendix G – Miscellaneous Support Functions for the details.
19. 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.
20. The CA Infrastructure should be built on on-premises 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. Service Providers must fully utilize our existing hardware. (The detail of hardware list in Appendix G – Hardware BOM)
21. 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:
    21.1. Reliable power supply

21.1.1. Dual feed PDU (Power Distribution Unit) on each rack.

21.1.2. Redundant UPS (Uninterruptible Power Supply).

21.1.3. Generator backup with sufficient fuel tanks.

21.2. Reliable air conditioning

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

21.2.2. Redundant chiller plants.

21.2.3. Generator backup.

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

21.2.5. Water leakage detection system.

21.3. Fire protection and suppression

21.3.1. Fire alarm system.

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

21.4. Security (24x7x365)

21.4.1. CCTV surveillance monitoring and recording.

21.4.2. Security guard patrol.

21.4.3. Physical security access control.

21.4.4. Pre-registration to access.

21.4.5. Security Operations Centre (SOC).

21.4.6. Network Operating Centre (NOC).

21.5. Connectivity

21.5.1. Dual lead-in.

21.5.2. Path diversity.

22. 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 Service Provider shall ensure that the design of the CA Infrastructure is still 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.
23. Verification of subscriber's identity through online platform.
24. HKIRC would provide a list of hardware (Hardware BOM would be listed in the Appendix G) for the infrastructure, service provider must fully utilize the HKIRC provided hardware before raising purchase request, additional cost submitted and will be included in the total costing. The total costing would be included in the final stage of costing marking scheme for total costing calculation.

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

4.2. Part B - Technical Support for Recognized Certification Authority (RCA) Application and Maintenance

1. HKIRC shall submit application to Certification Authority Recognition Office (CARO), Digital Policy Office (DPO) for recognition of the d-Cert (iAM Smart).
2. 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:
   2.1. Provisions of the Electronic Transactions Ordinance (Cap. 553) (ETO)
   2.2. The Code of Practice for RCA. Please refer to Code of Practice for Recognized Certification Authorities| Digital Policy Office for the details

4.3. Part C – Certification Authority (CA) Operation for iAM Smart

1. The Service Provider has to take all reasonable care in issuing iAM Smart Certificates to the Certificate Applicants or Certificate Subscribers and has to take all reasonable care to persons who may rely upon the iAM Smart Certificates (including without limitation to maintain CPS up to date, and make the Repository available for public access in accordance with the CPS). The detail requirements of iAM Smart are listed in section 4.3 point 4 and point 5.
   1.1. 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.
   1.2. 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.
   1.3. 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.
   1.4. 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 verify the identity of a person who applies for such a recognized certificate.
   1.5. 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).

1.6. Disclosure of Information - The Service Provider shall publish in the Repository or Repositories:

1.6.1. the CA Certificates that contain the public key corresponding to the private key used to digitally sign Certificates;

1.6.2. the suspension, revocation or non-renewal notice of the CA Certificates; and

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

1.6.4. 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.

1.6.5. 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.

1.6.6. 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.

1.6.7. 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.

1.6.8. The Service Provider should conduct all the verification of subscriber's identity through online platform, if applicable.

2. The Service Provider has to provide the generated Certificates (i.e. key pair) to DPO iAM Smart team and it's related system.
3. 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. The SLA and the details of specification requirements:

Category	Specification
iAM Smart-Cert Generation	• Monthly certificate issuance: **450,000 certificates** • Average response time: under ≤255 online CSR submissions per minute • Support issuance and deletion
OCSP (Online Certificate Status Protocol)	• Monthly OCSP response rate: **>300,000 responses** • Annual capacity: **85M requests** (~170 requests per minute on average) to return certificate status

Failover to Disaster Recovery platform (RTO)	• Estimated 30 mins
Failover to Disaster Recovery platform (RPO)	• 0 second
Production & Sandbox Site	• Local High Availability (Active-Active) • Sandbox not for Load test or Stress Test
DR Site	• Active-Standby design with 1:1 ratio to Production • in term of Processing Power
Testing Environment	• Require resilience • Support stress and load testing
Maximum certificate transactions / year	• ~6M
Maximum OCSP requests / month	• ~300k
CSR response time	• Less than 5 seconds
Maximum certificate transactions / minute	• ~250
Technical Support for iAM Smart Team	• 7x24 phone support (For DPO Only)
CA System connectivity's status with iAM Smart core system	• Real Time Online
Authentication methodology	• Support Single Sign ON (SSO) from iAM Smart systems

5. The Implementation and Support Team Structure and requirements for iAM Smart.

➢ General

- No single individual can perform more than one Key Role within the same team.
- Overlapping periods of experience will only be counted once. Total years are calculated by aggregate days divided by 365 up to the Proposal Closing Date.
- The following experience **will not be counted** time spent on:
    - Full-time undergraduate/postgraduate IT studies or sandwich training.
    - Sales or marketing of IT-related products/services.
    - Teaching IT-related subjects.

➢ Implementation Team Requirements

- **Minimum Commitment:** 1 member per each Key Role (as listed below), minimum **4 man-months** each. After the implementation completed, the implementation Team must continue to provide support till the DPO production final launch.
- **Language Requirement:** All members must read/write English & Chinese. **At least one (1) member** must speak fluent Cantonese, Putonghua, and English.

Key Role	Minimum Total IT Experience	Specific Project Experience Requirements	Core Responsibilities
Project Manager	**6+ years** IT experience	• **3+ years** PM experience (past 20 yrs). • **1+ year** PM experience in IT projects involving design/issuance of recognized digital certificates (past 10 yrs).	Overall management, QA, single point of contact.
CA Consultant	**4+ years** IT experience	• **2+ years** project experience (past 10 yrs) covering: Digital cert design **OR** seeking CDP recognition.	CA advice, certificate design, CDP recognition seeking, guidelines review.
CA Associate	**2+ years** IT experience	• **1+ year** project experience (past 10 yrs) covering: Producing System Docs (SA&D, testing), producing CPS, **OR** generating change proposals for recognized digital certificates.	Preparation of CPS and System Documents.
System Analyst	**4+ years** IT experience	• **2+ years** project experience (past 10 yrs) in RESTful API analysis/design/implementation, system specifications, and testing. • **1+ IT project** managing systems with **>1 million targeted users** (past 10 yrs).	System analysis, design, testing, and API-related development.

➢ System Support & Maintenance Team Requirements (required to provide 24 x 7 support)

- **Minimum Commitment:** 1 member per each Key Role (as listed below), minimum **24 man-months** each.
- **Language Requirement: ALL** proposed Maintenance Team members must read/write English & Chinese AND be able to communicate fluently in Cantonese, Putonghua, and English.

Key Role	Minimum	Specific Maintenance	Core Responsibilities

	Total IT/RCA Experience	Experience Requirements	
Maintenance Manager	**6+ years** IT experience	• **3+ years** project maintenance/support experience (past 20 yrs). • **1+ IT maintenance project** managing systems with **>1 million targeted users** (past 10 yrs).	Overall support/maintenance, incident escalation to Government, leading service recovery.
System Analyst	**4+ years** IT experience	• **2+ years** project experience (past 10 yrs) covering SA&D, API program development, System Documents preparation, testing, and system support/maintenance.	Supporting/maintaining APIs for integration with the **System**.
CA Support	**3+ years** CA experience	• **2+ years** project experience (past 10 yrs) covering: Resolving recognized digital certificate issuance problems **OR** helpdesk support for issuance/renewal/revocation.	CA support team leadership, issue/problem resolution.

4.4. Part D - System Implementation, Project Management and Documentation

The Service Provider 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 Service Provider)
1.	Project management • Project review meetings (at least once per month) • Ad-hoc project review meetings	• Project Implementation Plan (by phases, by timeline) • Cut-Over and Go-Live Plan • Change Management Plan • Post-Go-Live Support Plan • All Meeting Agendas • Meeting Minutes • Weekly and/or Monthly project progress reports

#	Project Activities/ Deliverables	Documentation (by the Service Provider)
2.	Project Initiation	• Project initiation document (PID)
3.	System Analysis and Design	• User requirement specification: o Business Requirements (BRD) o Functional Requirements (FRD) o Non-business/ System Requirements (SRS) o Requirement Traceability Matrix (RTM) o Database and Storage Requirements o Product Functions for UI/ UX • Gap analysis report: o Comparing the new system capabilities with user requirements o Identify the gap and develop business cases o Recommendations and Resolution to the gap • Mock-up/ prototype • Functional specifications: o Functional Data Flow Diagram (DFD) o Use Case Diagrams o User Interface o Performance o Manageability / Maintainability o System Interface / Integration o Security • Technical specifications: o System Architecture Diagram (SAD) o System Design Diagram (SDD) o Network Architecture Diagram (NAD) o RDBMS Database Design o Database Schema and Entity Relationship Diagram (ERD) o Database Data Dictionary o User Account Management o Password Management o Security Related Setup o System Interface and Connections o Integration with 3rd Parties Software and System
4.	Server Infrastructure Setup	• Network Diagram • System and Network Configuration
5.	Application Development	• Change Request:

#	Project Activities/ Deliverables	Documentation (by the Service Provider)
		○ Change Request Documentation (CR)
6.	Testing	• Test Plan, Test Scenarios
6.1.	Quality assurance (by the Service Provider)	• Quality Assurance Report
6.2.	System integration testing	• Test Cases, Test Scenarios ○ Cover all the functions for the CA System ○ 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 • Test Report ○ Report all the identified issues, status, and remedial actions for outstanding issues
6.3.	User acceptance testing	• Test Cases, Test Scenarios ○ Cover all the functions for the CA System ○ 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 • Test Report ○ Report all the identified issues, status, and remedial actions for outstanding issues
7.	Training	
7.1.	User training • For Operator and IT Department	• Training Plan and Schedule • User manual ○ Full workflow with step-by-step instructions, screenshots (and/or video clips) have to be provided • User training presentation materials (e.g. by PowerPoint, Word) • User training recordings
7.2.	System administration training • For IT Department	• System administration manual (for CA System and Infrastructure) ○ Full workflow with step-by-step instructions, screenshots (and/or video clips) have to be provided
7.3.	Operator training	• Certification Authority (CA) Operation Manual

#	Project Activities/ Deliverables	Documentation (by the Service Provider)
	• For Operator	○ Workflow of issuing, revoking, suspending, publishing Certificate ○ Workflow of verification of Certificate subscriber's identity ○ Workflow of delivering Certificate to subscriber ○ Full workflow with step-by-step instructions, screenshots (and/or video clips) have to be provided ○ 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 • The exercise will be conducted by a third-party service provider; and the vulnerabilities will be fixed by the Service Provider	• SRAA report(s) [by a third-party service provider]
11.	Privacy Impact Assessment (PIA) • The exercise will be conducted by a third-party service provider; and the remedial actions will be implemented by the Service Provider	• PIA report(s) [by a third-party service provider]
12.	Recognized Certification Authority 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.
14.	Critical Infrastructure	• The systems and operation required to fulfil the requirements of Critical Infrastructure Code Of Practices (CoP)

4.5. Part E - Information Security and Data Privacy Protection

Information security and data privacy are crucial to safeguard the digital assets of/ derived from the CA infrastructure. 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 Service Provider 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. 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: • After user acceptance testing (i.e. pre-production) Additional SRAA exercise(s) might be required if there are significant concerns or findings raised in the previous exercise(s).
2.2.	Code scanning shall be conducted and the Service Provider 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: • 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: • After user acceptance testing (i.e. pre-production) 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

#	Requirements
5.1.	The Service Provider 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 Service Provider 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. The Privileged Access Management (PAM) with Multi-Factor Authentication (MFA) is recommended. Service provide also can provide alternative security solution with detail specification.
      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. Application Life Cycle
   2.1. Project Initiation
      2.1.1. Ensure project requirements such as functions, which are operation or business focused.
      2.1.2. Ensure proper data classification involved to the website.

2.1.3. 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.

2.2. Feasibility Study

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

2.3. Systems Analysis & Design

2.3.1. 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.

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

2.3.3. Ensure appropriate technical and Organizational 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.

2.3.4. 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.

2.4. Implementation

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

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

2.4.3. 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.

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

2.4.5. Ensure source Code Review and Protection.

2.4.6. Ensure security risk assessment should be performed before the production launch.

2.4.7. 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.

2.5. Post-Implementation

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

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

2.5.3. 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.

2.5.4. Ensure security monitoring should be adopted to detect malicious activities.

2.5.5. Ensure an incident response and handling procedure should be defined.

2.5.6. Security risk assessments should be performed at least once every two years or after major changes.

2.6. Decommission

2.6.1. Ensure that the replacement is run properly and necessary migration has been performed such as data and user migration.

3. Security Guidelines and Standards:

3.1. ISO27001

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

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

4.6. Part F - System Maintenance and Support

#	Requirements
1.	Unlimited e-mail and telephone/ virtual conference support
1.1.	Support operating hours: • 7 days x 24 hours
2.	System bug fixing
2.1.	The Service Provider 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 Service Provider, 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 Service Provider 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 (i.e RCA, SRAA, PIA)
7.	HKIRC reserves the rights to do ad-hoc system enhancement or develop add-on components based on the Service Provider's 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. • All or a substantial portion of our mission critical data is at a significant risk of loss or corruption. • Have had a substantial loss of service. • Business operations have been completely halted. • Payment gateways have been completely not functioning
Major (Severity 2)	Major functionality is severely impaired. • 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. • A temporary workaround is available.
Minor (Severity 3)	Partial, non-critical loss of functionality of the software. • Impaired operations of some components, but allows the user to continue using the software. • Initial installation milestones are at minimal risk.
Cosmetic (Severity 4)	General usage questions. • 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 is 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 iAM Smart and other external systems through APIs or protocols
   iv. Customer-facing API for subscribing Certificate, verification of subscriber's identity, etc.

Severity	Response time	Resolution/ fixing time
1	30 minutes	4 hours
2	2 hours	6 hours
3	4 hours	48 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

4.7. Part G – Service Availability and Service Level

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. The new iAM Smart CA system should be connected with DPO (iAM Smart system) through API. (DPO will provide further API info upon contract award)
d. Customer-facing API 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.

For the details of CPS, please refer to the website of Hong Kong Post Office (iAM Smart-Cert Certification Practice Statement)

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 resilience; and local Active-Active resilience, i.e. minimum 4 nodes. If the cluster has more than half of the nodes 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 • 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. • 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.	• d-Cert (iAM Smart)
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
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 F - 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 F - System Maintenance and Support**

Services	Service Availability	Service Level
Performance and capacity management	• Perform capacity planning annually or when necessary.	• Please refer to **Part H – Service Capacity and Sizing** • The System capacity must be able to accommodate the demand (i.e. within ±10% deviation) within 12 months after annual planning • 99.99% Available Level for Core CA functions
Load Balancing and Resilience	• Local site load balancing has to be implemented to ensure the performance and minimize the downtime. • In case of one of the sites is down, i.e. the infrastructure is degraded, it has to be resumed promptly in order to meet the pledged system/ service availability. • 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. • 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

Services	Service Availability	Service Level
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.
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. • 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

4.8. Part H – Service Capacity and Sizing

1. CA Infrastructure Capacity

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:

The CA Infrastructure can also be scaled out to accommodate the demand of 6,000,000 Certificates per year ultimately:

5. Migration service for the existing CA operations for Personal Certificates, Organization certificates, Bank certificates to new CA Infrastructure (Optional)

1. Current CA infrastructure

HKIRC invites tenderers to submit proposals for the migration of the existing certificate system (covering personal, organisational, and encipherment server certificates, and any planned certificate types of the provided in the near future) to integrate with the proposed new CA Infrastructure.

HKIRC has established a Certification Authority (CA) infrastructure supporting these certificate types, and the underlying system is already in place. To meet the current certificate issuance volume requirements of this Project, the Service Provider shall assess and identify any additional hardware, software, and services required to support the migration of the existing CA system to the new CA Infrastructure. All such requirements must be clearly specified and included in the tender submission.

The migration must be carried out in compliance with applicable WebTrust requirements.

Certificate Types	**Number of Certificates per Year**
Issued/ renewed with manual processes (Maximum Yearly Capacity) include but not limited to the following cert types: a) Personal b) Organisational c) Encipherment d) Server e) Governmental f) Organisational Role g) Bank	~250,000
Accumulative & Renewal Certificate (around 6 years historical certificate) include but not limited to the following cert types: a) Personal b) Organisational c) Encipherment d) Server	~1,800,000

e) Governmental f) Organizational Role g) Bank	

2. System and Services Availability

The Service Provider has to meet the Availability Level (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 API for subscribing Certificate, verification of subscriber's identity, etc.

The Availability Level is a measure of the length of time of the 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 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-Standby 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 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 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.

3. <u>Services Availability/ Level Requirements:</u>

Services	Service Availability	Service Level
Help Desk Support (for Customer)	• 7 x 24 help desk support is required • 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. • 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 • e-Cert (Organisational) - 10 days • e-Cert (Encipherment) - 10 days • 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
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

Services	Service Availability	Service Level
Performance and capacity management	Perform capacity planning annually or when necessary.	Please refer to Part J – Service Capacity and Sizing The System capacity must be able to accommodate the demand (i.e. within ±10% deviation) within 12 months after annual planning 99.99% Available Level for Core CA functions
Load Balancing and Resilience	• Local site load balancing has to be implemented to ensure the performance and minimize the downtime. • In case of sites down, it has to be resumed promptly in order to meet the pledged system/ service availability. • 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. • 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. • For other requests requiring more efforts, an implementation plan has to be given on the next working day upon request.

6. Limitation of Liability and Indemnity

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

6.1. 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.

6.2. 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 6-year solid project management experience in the IT field.

6.3. 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.

6.4. Software Source Code Escrow

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

6.5. Sub-contracting/ Outsourcing

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

7. Information Security

The company submitting the proposal ("the company") shall acknowledge and agree that, if the company is selected as the Service Provider, 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.

8. 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 services.

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 services. 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.

9. Anti-collusion

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

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

(3) The Tenderer shall submit to the HKIRC a duly signed warranty in the form set out in Appendix 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 Service Provider.

10. Offering Advantages

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

connection with the tendering and execution of this contract.

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

11. Ethical Commitment

11.1. Prevention of bribery

(A) The Service Provider 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 Organization) solicit or accept any advantage as defined in the Prevention of Bribery Ordinance (Cap 201) in relation to the business of the Organization. The Service Provider 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 Organization. The Service Provider 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 Organization, solicit or accept any advantage, excessive hospitality, etc. in relation to the business of the Organization.

(B) The Service Provider 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 Organization.

11.2. Declaration of Interest

(C) The Service Provider shall require his directors and employees to declare in writing to the Organization 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 Service Provider 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 Service Provider shall require his agents and sub-contractors to impose similar restriction on their directors and employees by way of a contractual provision.

(D) The Service Provider 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 Service Provider shall require his agents and sub-contractors to impose similar restriction on their directors and employees by way of a contractual provision.

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

11.3. Handling of confidential information

(F) The Service Provider shall not use or divulge, except for the purpose of this Contract, any information provided by the Organization 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 Service Provider 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 Service Provider shall indemnify and keep indemnified the Organization against all loss, liabilities, damages, costs, legal costs, professional and other expenses of any nature whatsoever the Organization 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 Service Provider or his directors, employees, agents or sub-contractors.

11.4. Declaration of ethical commitment

(G) The Service Provider shall submit a signed declaration in a form (see Appendix B) prescribed or approved by the Organization 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 Service Provider fails to submit the declaration as required, the Organization shall be entitled to withhold payment until such declaration is submitted and the Service Provider 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 Service Provider and the sub-contractors employed for the performance of duties under this Contract are required to deposit with the Organization a copy of the internal guidelines issued to their staff.

12. Time Schedule

Milestone	Target Completion Date
Tender briefing	22-Jun-2026
Deadline for tender submission	10 July 2026, 23:59
Tender evaluation	July – Aug 2026
Tender Award	31-Aug-2026
DPO and HKIRC UAT	1-Feb-2027
Audit, including SRAA, RCA and related audits	15-Mar-2027
Target completion for implementation and ready for parallel run	1-Apr-2027

13. Payment Schedule

The following payment schedule is recommended but interested Service Providers 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 (if any), system integration and system live run	20%
4.	Passed iAM Smart Team testing (functional, load & Stress test)	35%
5.	System nursing and warranty (6-month)	30%

14. Elements of a Strong Tender

All submitted tender must follow the format as stated in Appendix C - HKIRC Proposal Requirements

Successful Service Provider 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 Service Provider.
- Excellent fit with the capabilities and facilities of HKIRC.
- Strong company and project management team.

The Service Provider selection criteria consist of 2 parts:

Technical	60%
Price	40%

The tender will be evaluated using a two-envelope method. The technical proposal and the price proposal shall be submitted in separate sealed envelopes.

The technical proposals will be opened and evaluated first, in accordance with the technical marking scheme set out in this document. Only those tenderers whose technical proposals achieve a passing score of more than 30 out of 50 will proceed to the price evaluation stage.

For any tenderer whose technical proposal fails to achieve the passing mark of over 30, the second envelope containing the price proposal will not be opened and the tender will not be considered further.

15. Service Agreement Negotiation and Signature

The service agreement will be drawn up between the selected Service Provider and HKIRC. HKIRC welcomes the Service Provider'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 negotiation with the next qualified Service Provider on the selection list.

16. HKIRC Contacts

HKIRC Contacts information

Contacts	
Hong Kong Internet Registration Corporation Limited Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong +852 2319 2303 - telephone +852 2319 2626 - fax http://www.hkirc.hk *If you are not sure about the appropriate person to call, the receptionist can help you.*	**Primary Contact:** **IT Manager** Frankie Chung +852 2319 3822 frankie.chung@hkirc.hk **Secondary Contact:** cft_dcert@hkirc.hk

Appendix A – Warranty

[start in next page]

To: Hong Kong Internet Registration Corporation Limited (HKIRC)

Dear Sir/Madam,

Warranty

(1) By submitting a tender, the Tenderer represents and warrants that in relation to the tender of Digital Certificate Project (Ref.: CFT-DCERT2-01):

(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 Service Provider 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 Service Provider 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 Service Provider)
(Name of the Signatory)
(Position of the Signatory)
(Date)

Appendix C – HKIRC Proposal Requirements

Proposal requirements	
Submission deadline	Please refer to Section 12 – Time Schedule, item no. 4 for the proposal submission deadline.
Hard copies	No Hard Copy is required
Electronic copy	Electronic copy is mandatory. It shall be sent by email to cft_dcert@hkirc.hk. For any inquiry, please contact to Frankie Chung (frankie.chung@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 – missions critical project experience
        (a) This part is to demonstrate experience in implementing projects involving mission critical infrastructure (e.g. financial sector, telecoms, government or other regulated sectors): based on relevance, scale and complexity of projects.
        (b) References should be cases over HKD 5 million successfully implemented in past five years. Suggested to provide 5 or more cases in total.
    - 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 (Tender Ref.: CFT-DCERT2-01)
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 Service Provider 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 Service Provider's financial situation.
- Brief description of the Service Provider'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 Service Provider 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. Service Provider shall provide relevant reference cases as mandatory information in their tender response. Such references should be closely related to digital certificate projects and should preferably demonstrate direct project experience in iAM Smart, or in similar digital certificate operations and/or support services

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

Please provide the details of background, including but not limited to:

- The structure of full-time technical team;
- Proven track record as system integrator (SI) with project of contract value successfully implemented in the past five years;
- Demonstrated experience in implementing projects involving critical infrastructure with relevance, scale and complexity of projects in the past five years;
- Each relevant named reference project involving certificate-related or similar security / trust infrastructure solutions in Hong Kong or overseas; and
- Relevance, recency (within the last five years), and similarity in scope will be taken into account when awarding marks.

6 Methodology

The Service Provider must describe the methods to be used, and briefly explain its advantage and disadvantage.

Please provide the details of the Solution architecture and design, including but not limited to:

- Overall system architecture, scalability, availability and security design
- Compliance with functional and non-functional requirements stated in the tender
- Clarity and completeness of design documentation (e.g. architecture diagrams, data flows, interfaces, security controls)

7 Project Management Methodology

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

Please provide the details of project methodology, including but not limited to:

- Overall system integration approach and project governance;
- Implementation and testing strategy;
- Operations model and procedures for certificate-related projects;
- Risk management, quality assurance and change control;
- Clear delineation between implementation/project team and ongoing operations/support team;
- Relevant qualifications and experience of key personnel in both implementation/project team and ongoing operations/support team;
- Availability of backup and succession arrangements; and
- Project team structure, which is providing a clear organisation chart and role descriptions, demonstrating that experienced team members

8 Understanding of our requirements

The Service Provider shall describe their understanding of our requirements. With the use of a table, the Service Provider 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 Service Provider should describe their knowledge and advice to ensure the success of this project/service or projects/services with similar nature.

Please provide the details of recommendations, including but not limited to:

- Proposing practical, innovative or risk-mitigation measures that are consistent with the project objectives.

10 Deliverable and Services level

The Service Provider 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.

Please provide the details, including but not limited to:

- A realistic, well-structured project plan that aligns with the required milestones and timeline;
- Provide 7x24 Network Operations Centre (NOC) and Security Operations Centre (SOC) support for the Data Processing Operations (DPO) environment, including incident response and monitoring; and
- Service Level Agreements (SLAs), response and resolution times, escalation procedures and reporting.

11 Implementation Time Table

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

Please provide the details of implementation schedule, including but not limited to:

- A realistic, well-structured project plan that aligns with the required milestones and timeline.

12 Commercial and Payment Terms

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

13 Innovative Suggestions

The Service Provider 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 Service Provider 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: • Integration with iAM Smart • Technical support for RCA application		
1.1.	Hardware	Core	5-year warranty
1.2.	Hardware Security Module (HSM)	Core	5-year warranty **HSM must fully ready to use the SM2 cryptographic algorithm**. Please list out the other detail specifications and other encryption algorithm support.
1.3.	Data Centre / on-premises	Core	For subscription based, please quote the fees for 4 years
1.4.	Software	Core	For subscription based, please quote the fees for 4 years
1.5.	Secure facilities	Core	For data centre hosting, please quote the fees for 4 years For Cloud, please estimate the subscription cost based on the initial sizing, and quote the fees for 4 years
1.6.	CA System (i.e. application) with project management and implementation services	Core	
1.7.	Verification of subscriber's identity by iAM Smart	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 • 2-year base + 2-year renewable contract • 2-year base contract: no fee increment is allowed

#	Item	Core/ Optional	Remarks
			• 2-year renewable contract: annual increment has to follow OR does not exceed the Consumer Price Index (Composite) of Hong Kong
3.	Certification authority (CA) operation, including: • Technical support for iAM Smart	Core	• Please quote the fees for 4 years, with yearly breakdown • 2-year base + 2-year renewable contract • 2-year base contract: no fee increment is allowed • 2-year renewable contract: annual increment has to follow the Consumer Price Index (Composite) of Hong Kong • 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: • Integration with iAM Smart • Technical support for RCA application	**Sub-total:**		[redacted]				
1.1.	Hardware	Core						One-off with 5-year warranty
1.2.	Hardware Security Module (HSM)	Core						One-off with 5-year warranty **HSM must fully ready to use the SM2 cryptographic algorithm.** Please list out the other detail specifications and other encryption algorithm support.
1.3.	Cloud Service / Data Centre / on-premises	Core						4-year subscription

				Breakdown (HK$)				
#	Item	Core/ Optional	HK$	Year 1	Year 2	Year 3	Year 4	Remarks
1.4.	Software	Core						Perpetual + 4-year warranty OR 4-year subscription
1.5.	Secure facilities	Core						4-year data centre rental AND/OR 4-year Cloud subscription
1.6.	CA System (i.e. application) with project management and implementation services	Core						One-off
1.7.	Verification of subscriber's identity by iAM Smart	Core						One-off
1.8.	ITAI alternative solution	Optional						H/W: one-off with 5-year warranty S/W: Perpetual + 4-year warranty OR 4-year subscription

				Breakdown (HK$)				
#	**Item**	**Core/ Optional**	**HK$**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Remarks**
2.	System support and maintenance for CA infrastructure	Core						4-year service 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.
3.	Certification authority (CA) operation, including: • Technical support for iAM Smart	Optional						4-year service • 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 Service Providers that their participation and conformance in these measures and controls are essential contractual obligations.

The original Policy applies to HKIRC's employees, Service Providers, and third-party users. However, a potential Service Provider may interpret the clauses up to their roles and responsibilities only. Nonetheless, the keyword "Service Providers" hereby refers to all relevant staff of the Service Provider and of any other subcontractors under the Service Provider's purview. Herein, HKIRC would also set the expectation of any potential Service Providers 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.

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

shall state their and the Organization's responsibilities for information security.

7.2 DURING EMPLOYMENT

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

7.3.2 All employees, Service Providers 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, Service Providers 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 Service Providers 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. 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. 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 : a. Generated certificates; b. Certificate profiles; c. Certificate Revocation Lists (CRL(s)); 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 : d. System configuration parameters; e. Operating users access control data; f. Application data; g. Subscriber and subscription information; h. Certificates information; i. Payment records; j. Notification information and records; 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. 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. 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. 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. 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. 3. The backup management server should provide the centralised backup management of backup jobs on the different servers installed with backup management agents. 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. 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. 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 – 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

Appendix G – Hardware BOM

Item	Part #	Description	Qty
		Quoted with 5 years Maintenance, including 7x24 with Onsite support Service	
		Each Item warranty start upon the delivery, e.g. hardware warranty /maintenance start upon the hardware	
		Active Passive Design - Infra for Primary and Secondary Sites	
		Hypervisor Server or VM Hosts for pxpkvm01/02/03 & pxrkvm01: (3 x Primary Site, 1 x Secondary Site)	
1	3700025283504.12	**Dell PowerEdge R770 Server (5 years MA)**	4
		per Unit BoM Included:	
		Components	
Base		PowerEdge R770 Server [Hypervisor Server]	1
Chassis Configuration		2.5" Chassis with up to 16 SAS4/SATA Drives, Smart Flow, Front PERC 12 (H965i)	1
Processor		Intel Xeon 6 Performance 6520P 2.4G, 24C/48T, 24GT/s, 144M Cache, Turbo, (210W) DDR5-6400	1
Thermal Configuration		Heatsink for 2 CPU configuration (CPU more than 200W and less than 250W)	1
Memory Configuration Type		Performance Optimized	1
Memory DIMM Type and Speed		6400MT/s RDIMMs	1
Memory Capacity		32GB RDIMM, 6400MT/s, Dual Rank	16
RAID Configuration		No RAID	1
RAID Controller		PERC H965i Controller, Front, DCMHS	1
Hard Drives		480GB SSD SATA Read Intensive 6Gbps 512e 2.5in Hot-plug AG Drive, 1 DWPD	2
BIOS and Advanced System Configuration Settings		Performance BIOS Settings	1
Fans		PowerEdge 2U High Performance Silver Fan	1
Power Supply		Dual, Redundant(1+1), Hot-Plug MHS Power Supply,1100W MM	1
Power Cords		Power Cord - C13, 2M, 250V, 10A (UK, Malaysia, Singapore, HK, Brunei, DDD)	2
PCIe Riser		Riser Config 6-1, Rear Half Length, 4x16 FH Slots (Gen5), 1x8/1x16 OCP (Gen5), 2nd OCP x16 (Gen5)	1
Motherboard		PowerEdge R770 Motherboard for RTS1.2, ROW	1
OCP 3.0 Network Adapters		Broadcom 57412 Quad Port 10GbE Base-T adapter, OCP 3.0 NIC +Sec	2
OCP 3.0 Accessories		No OCP Blanks or Cables Required	1
Bezel		Dell Luggage Tag, R770	1
Bezel		PowerEdge 2U Standard Bezel	1
Boot Optimized Storage Cards		Rear Filler Blank for BOSS/OCP	1
Embedded Systems Management		iDRAC10, Enterprise 17G	1
Embedded Systems Management		Dell Connectivity Client - Enabled	1
Embedded Systems Management		Dell Connectivity Module 17G	1
BMC Password		iDRAC Legacy Password for OCP cards	1
Rack Rails		ReadyRails Sliding Rails (B21)	1
SHIPPING		PowerEdge Shipping APCC, CCC, ICC	1
SHIPPING		PowerEdge R770 Shipping, APCC,CCC4,ICC	1
Shipping Material		PowerEdge 2U Shipping Material	1
Regulatory		PowerEdge CCC, No CE Label Marking	1
GPU/FPGA/Acceleration Cables		No Cables Required	1
Additional Processor		Intel Xeon 6 Performance 6520P 2.4G, 24C/48T, 24GT/s, 144M Cache, Turbo, (210W) DDR5-6400	1
Additional Processor		Additional Processor Selected	1
Acceleration Cards Cables		No Cables Required	1

	KVM	Blank Left Ear Module		1
		Software		
	Advanced System Configurations	UEFI BIOS Boot Mode with GPT Partition		1
	Operating System	No Operating System		1
	OS Media Kits	No Media Required		1
	Embedded Systems Management	Secure Enterprise Key Manager License 3.0		1
	Embedded Systems Management	Secured Component Verification		1
	Dell Secure Onboarding	Dell Secure Onboarding Client 17G - Disabled		1
		Support Service		
	Dell Services: Hardware Support	Dell ProSupport with 4-Hour Onsite Service Initial (7x24x4), 60 Month(s)		1
	Keep Your Hard Drive for Enterprise Services	Keep Your Hard Drive For Enterprise, 60 Month(s)		1
		Hypervisor Server or VM Hosts for pxpkvm11/12/13 & pxrkvm11: (3 x Primary Site, 1 x Secondary Site)		
2	**3700025283504.12**	**Dell PowerEdge R770 Server (5 years MA)**		**4**
		per Unit BoM Included:		
		Components		
	Base	PowerEdge R770 Server		1
	Chassis Configuration	2.5" Chassis with up to 24 Drives (16 SAS4/SATA + 8 NVMe Direct), Front PERC 12 (H965i)		1
	Processor	Intel Xeon 6 Performance 6520P 2.4G, 24C/48T, 24GT/s, 144M Cache, Turbo, (210W) DDR5-6400		1
	Thermal Configuration	Heatsink for 2 CPU configuration (CPU more than 200W and less than 250W)		1
	Memory Configuration Type	Performance Optimized		1
	Memory DIMM Type and Speed	6400MT/s RDIMMs		1
	Memory Capacity	32GB RDIMM, 6400MT/s, Dual Rank		16
	RAID Configuration	No RAID		1
	RAID Controller	PERC H965i Controller, Front, DCMHS		1
	Hard Drives	480GB SSD SATA Read Intensive 6Gbps 512e 2.5in Hot-plug AG Drive, 1 DWPD		2
	BIOS and Advanced System Configuration Settings	Performance BIOS Settings		1
	Fans	PowerEdge 2U High Performance Silver Fan		1
	Power Supply	Dual, Redundant(1+1), Hot-Plug MHS Power Supply,1100W MM		1
	Power Cords	Power Cord - C13, 2M, 250V, 10A (UK, Malaysia, Singapore, HK, Brunei, DDD)		2
	PCIe Riser	Riser Config 6-1, Rear Half Length, 4x16 FH Slots (Gen5), 1x8/1x16 OCP (Gen5), 2nd OCP x16 (Gen5)		1
	Motherboard	PowerEdge R770 Motherboard for RTS1.2, ROW		1
	OCP 3.0 Network Adapters	Broadcom 57412 Quad Port 10GbE Base-T adapter, OCP 3.0 NIC +Sec		2
	OCP 3.0 Accessories	No OCP Blanks or Cables Required		1
	Bezel	Dell Luggage Tag, R770		1
	Bezel	PowerEdge 2U Standard Bezel		1
	Boot Optimized Storage Cards	Rear Filler Blank for BOSS/OCP		1
	Embedded Systems Management	iDRAC10, Enterprise 17G		1
	Embedded Systems Management	Dell Connectivity Client - Enabled		1
	Embedded Systems Management	Dell Connectivity Module 17G		1
	BMC Password	iDRAC Legacy Password for OCP cards		1
	Rack Rails	ReadyRails Sliding Rails (B21)		1
	SHIPPING	PowerEdge Shipping APCC, CCC, ICC		1
	SHIPPING	PowerEdge R770 Shipping, APCC,CCC4,ICC		1

	Shipping Material	PowerEdge 2U Shipping Material		1
	Regulatory	PowerEdge CCC, No CE Label Marking		1
	GPU/FPGA/Acceleration Cables	No Cables Required		1
	Additional Processor	Intel Xeon 6 Performance 6520P 2.4G, 24C/48T, 24GT/s, 144M Cache, Turbo, (210W) DDR5-6400		1
	Additional Processor	Additional Processor Selected		1
	Acceleration Cards Cables	No Cables Required		1
	KVM	Blank Left Ear Module		1
		Software		
	Advanced System Configurations	UEFI BIOS Boot Mode with GPT Partition		1
	Operating System	No Operating System		1
	OS Media Kits	No Media Required		1
	Embedded Systems Management	Secure Enterprise Key Manager License 3.0		1
	Embedded Systems Management	Secured Component Verification		1
	Dell Secure Onboarding	Dell Secure Onboarding Client 17G - Disabled		1
		Support Service		
	Dell Services: Hardware Support	Dell ProSupport with 4-Hour Onsite Service Initial (7x24x4), 60 Month(s)		1
	Keep Your Hard Drive for Enterprise Services	Keep Your Hard Drive For Enterprise, 60 Month(s)		1
		Backup Server for lxrbak01 & lxrbak01: (1 x Primary Site, 1 x Secondary Site)		
3	**3700025283504.12**	**PowerEdge R570 Server, Enterprise (5 year MA)**		**2**
		per Unit BoM Included:		
		Components		
	Base	PowerEdge R570 Server, Enterprise [backup server]		1
	Chassis Configuration	3.5" Chassis with up to 12 SAS4/SATA Drives, PERC 12 (H965i or H365i)		1
	Processor	Intel Xeon 6 Performance 6741P 2.5G, 48C/96T, 288M Cache, Turbo, (300W) DDR5-6400		1
	Thermal Configuration	Heatsink for 1 CPU Configuration (CPU greater than 250W)		1
	Memory Configuration Type	Performance Optimized		1
	Memory DIMM Type and Speed	6400MT/s RDIMMs		1
	Memory Capacity	16GB RDIMM 6400Mt/s, Single Rank		4
	RAID Configuration	No RAID		1
	RAID/Internal Storage Controllers	H965i Adapter Full Height		1
	Hard Drives	16TB Hard Drive SAS ISE 12Gbps 7.2K 512e 3.5in Hot-Plug, AG Drive		5
	BIOS and Advanced System Configuration Settings	Power Saving Dell Active Power Controller		1
	Fans	PowerEdge 2U High Performance Gold Fan		1
	Power Supply	Dual,Redundant(1+1),Hot-PlugMHSPowerSupply,1100WMM(100-240Vac)		1
	Power Cords	Jumper Cord - C13/C14, 2M, 250V, 10A (EU, TW, APCC countries except ANZ)		2
	PCIe Riser	Riser Config 10, Rear Full Height 1x16 Onboard OCP, 1x16 FLOP OCP, 3x16 FH (Gen5)		1
	Motherboard	PowerEdge R570 Motherboard, ROW		1
	Multi Selection Network Adapter	Broadcom 57412 Quad Port 10GbE Base-T adapter, OCP 3.0 NIC +Sec		2
	OCP 3.0 Accessories	No OCP Blanks or Cables Required		1
	Cables	No Cables Required		1
	GPU/FPGA/Acceleration Cables	No Cables Required		1
	Bezel	No Bezel		1
	Bezel	Dell Luggage Tag, R570		1

	Boot Optimized Storage Cards	BOSS-N1 controller card + with 2 M.2 480GB (RAID 1) (22x80)	1
	Embedded Systems Management	iDRAC10, Enterprise 17G	1
	Embedded Systems Management	Dell Connectivity Client - Enabled	1
	Embedded Systems Management	Dell Connectivity Module 17G	1
	KVM	Blank Left Ear Module	1
	BMC Password	iDRAC Factory Generated Password for OCP cards	1
	Rack Rails	2U Combo Drop-In/Stab-In Rails (B22)	1
	SHIPPING	PowerEdge Shipping APCC, CCC, ICC	1
	SHIPPING	R570 Shipping, APCC, CCC4, ICC	1
	Shipping Material	PowerEdge 2U Shipping Material	1
	Regulatory	PowerEdge CCC, No CE Label Marking	1
	Software	Software	
	Advanced System Configurations	UEFI BIOS Boot Mode with GPT Partition	1
	Operating System	No Operating System	1
	OS Media Kits	No Media Required	1
	Embedded Systems Management	Secure Enterprise Key Manager License 3.0	1
	Embedded Systems Management	Secured Component Verification	1
	Dell Secure Onboarding	Dell Secure Onboarding Client 17G - Disabled	1
	Service	Support Service	
	Dell Services: Hardware Support	ProSupport with 4-Hour Onsite Service Initial (7x24x4), 60 Month(s)	1
	Keep Your Hard Drive for Enterprise Services	Keep Your Hard Drive For Enterprise, 60 Month(s)	1
		Isolated Core (1 x Primary Site, 1 x Secondary Site)	
4	**3700025283504.12**	**PowerEdge R570 Server, Enterprise (5 year MA)**	**2**
		per Unit BoM Included:	
		Components	
	Base	PowerEdge R570 Server, Enterprise [Isolated Core (Prod & DR):]	1
	Chassis Configuration	2.5" Chassis with up to 8 NVMe (G4), PERC 12 (H965i)	1
	Processor	Intel Xeon 6 Performance 6517P 3.2G, 16C/32T, 24GT/s, 72M Cache, Turbo, (190W) DDR5-6400	1
	Thermal Configuration	Heatsink for 1 CPU Configuration (CPU greater than 185W and less than 250W)	1
	Memory Configuration Type	Performance Optimized	1
	Memory DIMM Type and Speed	6400MT/s RDIMMs	1
	Memory Capacity	16GB RDIMM 6400Mt/s, Single Rank	4
	RAID Configuration	C31, No RAID with NVMe and front PERC	1
	RAID/Internal Storage Controllers	PERC H965i Controller, Front, DCMHS	1
	Hard Drives	No Hard Drive	1
	Hard Drives (PCIe SSD/Flex Bay)	1.6TB Enterprise NVMe Mixed Use AG Drive U.2 with carrier	2
	BIOS and Advanced System Configuration Settings	Power Saving Dell Active Power Controller	1
	Fans	PowerEdge Sirocco Fan - Non-DW GPU, Non-3.5" Config, Non-32xE3 Config	1
	Power Supply	Dual,Redundant(1+1),Hot-PlugMHSPowerSupply,1100WMM(100-240Vac)	1
	Power Cords	Jumper Cord - C13/C14, 2M, 250V, 10A (EU, TW, APCC countries except ANZ)	2
	PCIe Riser	Riser Config 5, Rear Full Height 2x16 FH (Gen5), 1x16 FLOP OCP, 1x16 Onboard OCP	1
	Motherboard	PowerEdge R570 Motherboard, ROW	1
	Multi Selection Network Adapter	Broadcom 57412 Quad Port 10GbE Base-T adapter, OCP 3.0 NIC +Sec	2
	OCP 3.0 Accessories	No OCP Blanks or Cables Required	1

	Cables	No Cables Required	1
	GPU/FPGA/Acceleration Cables	No Cables Required	1
	Bezel	No Bezel	1
	Bezel	Dell Luggage Tag, R570	1
	Boot Optimized Storage Cards	BOSS-N1 controller card + with 2 M.2 480GB (RAID 1) (22x80)	1
	Embedded Systems Management	iDRAC10, Enterprise 17G	1
	Embedded Systems Management	Dell Connectivity Client - Enabled	1
	Embedded Systems Management	Dell Connectivity Module 17G	1
	KVM	Blank Left Ear Module	1
	BMC Password	iDRAC Factory Generated Password for OCP cards	1
	Rack Rails	2U Combo Drop-In/Stab-In Rails (B22)	1
	SHIPPING	PowerEdge Shipping APCC, CCC, ICC	1
	SHIPPING	R570 Shipping, APCC, CCC4, ICC	1
	Shipping Material	PowerEdge 2U Shipping Material	1
	Regulatory	PowerEdge CCC, No CE Label Marking	1
		Software	
	Advanced System Configurations	UEFI BIOS Boot Mode with GPT Partition	1
	Operating System	No Operating System	1
	OS Media Kits	No Media Required	1
	Embedded Systems Management	Secure Enterprise Key Manager License 3.0	1
	Embedded Systems Management	Secured Component Verification	1
	Dell Secure Onboarding	Dell Secure Onboarding Client 17G - Disabled	1
		Support Service	
	Dell Services: Hardware Support	Dell ProSupport with 4-Hour Onsite Service Initial (7x24x4), 60 Month(s)	1
	Keep Your Hard Drive for Enterprise Services	Keep Your Hard Drive For Enterprise, 60 Month(s)	1
		Dell Server Network Card	
5		**Dell Broadcom 57412 Quad Port 10GbE Base-T adapter, OCP 3.0 NIC +Sec** ****4 pcs Network Card ready for server Uprgade**	4
		System Management PC (1 x Primary Site, 1 x Secondary Site)	
6	**A1LH4PA#AB5**	**HP Pro SFF 400 G9, Q670 Chipset, Intel i5-14500 vPro Essential, 16GB DDR5, 512GB M.2 PCIe NVMe SSD, DVDRW, 9*USB Ports, 1*DP+2*HDMI, 1*Serial, Intel AX211 Wifi 6+BT, Eng USB KB/Mouse, Int-Speaker, W11P, 5 years , On-site Wty**	2
		NetApp SAN Storage (1 x Primary site):	
7	441404	**NetApp Prod_FQ_1xASAA20_8x10GbRJ45_ports_10x3.84TB_ONTAPOne_5yr_LSC_NRD_4hr_Del** **- Usable: 22.46TiB** ****Per Unit BoM Including:**	1
	ASA-A20-001	ASA A20 HA System	2
	ASA-A20A-100-C	ASA A20 HA System,-C	1
	X4025A-2-A-C	Drive Pack 2X3.8TB,NVMe4,SED,-C	5
	X60132A-C	IO Module,4PT,10/25GbE,-C	2

	X60133A-C	IO Module,4PT,10GBASE-T,RJ45,-C	2
	X6562-R6-N-C	Cable,Ethernet,5m RJ45 CAT6,-C	8
	X66240A-05-N-C	Cable,25GbE,SFP28-SFP28,Cu,0.5m,-C	2
	X66250-5-N-C	Cable,LC-LC,OM4,5m,-C	4
	X6589-N-C	SFP+Optical 10Gb Shortwave,-C	4
	X5532A-N-C	Rail,4-Post,Thin,Rnd/Sq-Hole,Sm,Adj,24-32,-C	1
	X800C-R6-C	Power Cable,UK and Ireland,-C,R6	2
	X97602A-C	Power Supply,1600W,Titanium,-C	2
	DATA-AT-REST-	Data at Rest Encryption Capable Operating Sys	2
	SW-ONTAPO-FLASH-ASA-	SW,ONTAP One Package,Per TB,Flash,ASA-A20,-C	38
	CS-G1A-PARTNER-P-R	SupportEdge PartnerSelect - 60 months	1
	CS-4HR-DELIVERY-A-P-R	4hr Parts Delivery, LSC - 60 months	1
	CS-NON-RETURNABLE-	Non-Returnable Drives (HDDs,SSDs) - 60 months	1
		NetApp SAN Storage (1 x Secondary site):	
8	441426	**NetApp DR_FQ_1xASAA20_8x10GbRJ45_ports_10x1.92TB_ONTAPOne_5yr_LSC_NRD_4hr_Del**	**1**
		- Usable: 10.85TiB	
		**Per Unit BoM Including:	
	ASA-A20-001	ASA A20 HA System	2
	ASA-A20A-100-C	ASA A20 HA System,-C	1
	X4024A-2-A-C	Drive Pack 2X1.92TB,NVMe4,SED,-C	5
	X60132A-C	IO Module,4PT,10/25GbE,-C	2
	X60133A-C	IO Module,4PT,10GBASE-T,RJ45,-C	2
	X6562-R6-N-C	Cable,Ethernet,5m RJ45 CAT6,-C	8
	X66240A-05-N-C	Cable,25GbE,SFP28-SFP28,Cu,0.5m,-C	2
	X66250-5-N-C	Cable,LC-LC,OM4,5m,-C	4
	X6589-N-C	SFP+Optical 10Gb Shortwave,-C	4
	X5532A-N-C	Rail,4-Post,Thin,Rnd/Sq-Hole,Sm,Adj,24-32,-C	1
	X800C-R6-C	Power Cable,UK and Ireland,-C,R6	2
	X97602A-C	Power Supply,1600W,Titanium,-C	2
	DATA-AT-REST-	Data at Rest Encryption Capable Operating Sys	2
	SW-ONTAPO-FLASH-ASA-	SW,ONTAP One Package,Per TB,Flash,ASA-A20,-C	19
	CS-G1A-PARTNER-P-R	SupportEdge PartnerSelect - 60 months	1
	CS-4HR-DELIVERY-A-P-R	4hr Parts Delivery, LSC - 60 months	1
	CS-NON-RETURNABLE-	Non-Returnable Drives (HDDs,SSDs) - 60 months	1
		KVM: (1 x Primary Site, 1 x Secondary Site)	
9		**Aten CL5716im / 16-Port 17" LCD KVM switch over IP (1Local & 1Remote user)**	**2**
9.1		**Aten 2L-5202U / 1.8m VGA USB KVM cable**	**16**
		Hyper Hypervisor License for Primary Site and Secondary Site	
10	**DG7GMGF0PWHC:0003**	**Windows Server 2025 Standard - 16 Core License Pack**	**30**
		(Perpetual License)	
		- Windows Server License for Prod & DR:	
		6x Production Hyper-V (48 Core) – Allow 12 Windows Guest OS	
		2x DR Hyper-V (48 Core) – Allow 4 Windows Guest OS	
		2x Backup Server (48 Core) – 2 Physical Veeam Server	

		'= 480 / 16 Core = 30 Windows Standard License (16-Core)	
		Backup License for Primary Site and Secondary Site	
11	V-FDNVUL-0I-SU3YP-00	**Veeam Data Platform Foundation Universal Subscription License. Includes Enterprise Plus Edition features. 10 instance pack. Production (24/7) Support. (5 years)** **Estimated with 60 x VM Guest OS to Backup for DC1 & DC2	6
		NAS for Syslog Archiaving (1 x Primary Site, 1 x Secondary Site)	
12	HD-RS822+ {HD-HA53116	**Synology RS822+ NAS** - 3 x Synology Enterprise Series HAT5310-16T 7200rpm SATA HDD - 1 x Synology Rail kit- Sliding RKS02 - Uprgade to 5 years MA	2
		External USB Disk for Off-site Backup Copy	
13		**External USB Disk - 2T**	3
		Infra shopping List for UAT#1 and UAT2	
14		**NetApp Storage (1 x NetApp for UAT#1 & UAT#2)**	
	441479	**NetApp UAT_FQ_1xAFFA20_8x10GbRJ45_ports_6x1.92TB_ONTAPOne_5yr_LSC_NRD_4hr_Del** **- Usable: 4.22TiB**	1
		**Per Unit BoM Including:	
	AFF-A20-001	AFF A20 HA System	2
	AFF-A20A-100-C	AFF A20 HA System,-C	1
	X4024A-2-A-C	Drive Pack 2X1.92TB,NVMe4,SED,-C	3
	X60132A-C	IO Module,4PT,10/25GbE,-C	2
	X60133A-C	IO Module,4PT,10GBASE-T,RJ45,-C	2
	X6562-R6-N-C	Cable,Ethernet,5m RJ45 CAT6,-C	8
	X66240A-05-N-C	Cable,25GbE,SFP28-SFP28,Cu,0.5m,-C	2
	X66250-5-N-C	Cable,LC-LC,OM4,5m,-C	4
	X6589-N-C	SFP+Optical 10Gb Shortwave,-C	4
	X5532A-N-C	Rail,4-Post,Thin,Rnd/Sq-Hole,Sm,Adj,24-32,-C	1
	X800C-R6-C	Power Cable,UK and Ireland,-C,R6	2
	X97602A-C	Power Supply,1600W,Titanium,-C	2
	DATA-AT-REST-	Data at Rest Encryption Capable Operating Sys	2
	SW-ONTAPO-FLASH-A20-C	SW,ONTAP One Package,Per TB,Flash,A20,-C	11
	CS-G1A-PARTNER-P-R	SupportEdge PartnerSelect - 60 months	1
	CS-4HR-DELIVERY-A-P-R	4hr Parts Delivery, LSC - 60 months	1
	CS-NON-RETURNABLE-	Non-Returnable Drives (HDDs,SSDs) - 60 months	1
		Backup License FOR UAT#1 and UAT#2	
15	V-FDNVUL-0I-SU3YP-00	**Veeam Data Platform Foundation Universal Subscription License. Includes Enterprise Plus Edition features. 10 instance pack. Production (24/7) Support. (5 years)** **Estimated with 60 x VM Guest OS to Backup for UAT#1 and UAT#2	6

		Hyper Hypervisor License for DC1 & DC2	
16	DG7GMGF0PWHC:0003	**Windows Server 2025 Standard - 16 Core License Pack** since Customer is sharing the UAT / DEV, the hyper-V is 24x2x6/16 = 18x Windows 2025 Standard, and add 2x Backup (Perpetual License) - Windows Server License for UAT#1 & UAT#2 6x UAT1 Hyper-V (48 Core) – Allow 12 Windows Guest OS 2x UAT2 / Dev Hyper-V (48 Core) – Allow 4 Windows Guest OS 2x UAT Backup Server (24 Core) – 2 Physical Veeam Server '= 432 / 16 Core = 27 Windows Standard License (16-Core)	**27**
		Active Passive Design - Professional Service	
		Implementation service:	
17		**Professional Service: Hyper-V farm Infrastructure implementation (Active Passive Design)** - Detailed Service Scope pleaes refer to the technical Propsoal	**1**
		Ongoing Support Service SYSTEM MAINTENANCE AND SUPPORT SERVICES	
18		**Profressional SYSTEM MAINTENANCE AND SUPPORT SERVICES for the Project (Active Passive Design)** **Detailed SM&S Scope please refer to technical propsoal - Per monthly service Original cost = HK$30,000 / per month for this Project - The Project Team specially free this service to the Customer for the agreed service period - Including the System patching service alongside and assistance to Customer for the on-going Maintenance	1
19		**One off Special Discount Support to HKIRC for the New Environment implementation Project** althrough with special discount support for this project, but the Project team will be still covering below service: - Migration Existing Production Site to New Production Site - Migration Existing DR Site to New DR Site - Change Existing IP / Hostname of the Production Site to UAT Site - Change Existing IP / Hostname of DR Site to DEV Site - Assist HSM Vendor For Switchover - Verify the Web / Database Migration Status -5 years support service to the add on 2 x sites after the migration	**1**
		Active Passive Design - OpenText for Monitoring	
		Opentext for Infra (Server + Network) Monitoring Tool	
20		**Opentext for Infra (Server + Network) Monitoring Tool - 5 YR License** ** For this Project new Server + network monitoring , including - OpenText AI monitoring tool for 100 servers Monitoring (5 years license) - OpenText AI monitoring tool for 30 network devices Monitoring (5 years License)	**1**

Item	Part #	Description	Qty
		* Quoted with 5 years Maintenance, including 7x24 with Onsite support Service * Each Item warranty start upon the delivery, e.g. hardware warranty /maintenance start upon the * hardware delivery	
		Active Passive - Primary and Secondary Sites Network Devices	
		Internet Facing Firewall - Sangfor Firewall (2 x Primary Site and 1 x Secondary site)	
1.0	NSF1050A	**Sangfor NETWORK SECURE NSF-1050A-I Firewall (5 years SNS)** - Per Unit BoM Including	3
1.1	NSF1050A	NSF-1050A-I, Athena NGFW hardware appliance. Desktop, 8 x GE RJ45, 2 x SFP, 128GB SSD. Single AC power supply.	1
1.2	PM-1050A-5Y	NSF-1050A-I, Premium Bundle(SSL VPN, Site-to-Site IPsec VPN, Secure SD-WAN, Stateful Firewall, Bandwidth Management, URL Filtering, Application Control, IPS, Botnet Prevention, Email Security, SOC Lite, Basic Security Reporter, Engine Zero, Neural-X), 5 Years.	1
1.3	HSDS-1050A-1Y	NSF-1050A-I, Network Secure, Same Day Shipment Hardware Service, 5 Year.	1
1.4	SUS-1050A-1Y	NSF-1050A-I, Software Upgrade Services, 5 year.	1
1.5	TSS-1050A-1Y	NSF-1050A-I, 24*7 Technical Support Services, 5 year.	1
1.6	SANGFOR-SWAP-7X24-NSF1050A	7x24x4 swapping service during non-Business Hour, Customer shall provide configuration backup file(s) for hardware recovery. - 5 years	1
		****Remark For the Intrusion detection System Solution (IDS) :** For Project requirement of an IDS for the external firewall, we propose Sangfor NGFW, as it includes a fully integrated Intrusion Prevention System (IPS) that also delivers comprehensive IDS capabilities. Sangfor's IPS continuously monitors inbound and outbound traffic using signature-based and behavior-based detection to identify potential threats, suspicious activities, and attack patterns in real time. Unlike standalone IDS solutions, the built-in IPS not only detects intrusions but can automatically block, prevent, and respond to threats at the firewall level, reducing attack dwell time and operational complexity. This approach provides customer with stronger perimeter protection, simplified management through a single platform, and cost efficiency by eliminating the need for a separate external IDS appliance.	
		Internal Facing firewall - PA (4 x Primary Site and 2 x Secondary site)	
2.0	PAN-PA-1410	**Palo Alto Networks 1410 (with 5 years Support & Subscription)** - Per Unit BoM Including:	6
2.1	PAN-PA-1410	**Palo Alto Networks PA-1410**	1
2.2	PAN-SVC-BKLN-1410-3YR	PA-1410, Partner enabled premium support,	1
2.3	PAN-PA-1410-BND-PRECISIONAI-3YR	PA-1410, Precision AI Network Security Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security, Advanced SD-WAN and Device Security),	1
2.4	PAN-PWR-450W-AC	PA-3400,PA-1400, ION 5200 and ION 9200 450W spare power supply	1
2.5	PAN-1RU-RACK-KIT-4POST	Palo Alto Networks 4-Post rack mount kit for 1U PA-1400	1
2.6	BD-SWAP-PRE	Swapping Service - 24x7x4 (Including On-site Labour)	1
		Network Switch (Total 12 Set Switch)	
		Core Switch (H3C S5590-24UXMC-EI L3) - 2 set for Primary Site, 1 set for Secondary site	
3.0	H3C S5590-24UXMC-EI	**H3C S5590-24UXMC-EI L3 Ethernet Switch, per Switch BoM Including:** - Per Unit BoM Including: H3C S5590-24UXMC-EI L3 Ethernet Switch with 24*100M/1G/2.5G/5G/10GBASE-T PoE++ Ports and 1* Slot, Without Power Supplies; 8-Port 10G SFP Plus Interface Module; SFP+ Cable 1.2m; 2 * H3C,PSR600-54A-B,600W/AC PoE Power Supply; 2 * H3C Fan Module (Fan Panel Side Exhaust Airflow); 5 * Network Product Onsite Service 7×24×4 (5 yrs MA)	3
		Zone Access Switch (H3C S5590-28TSXC-EI L3) - 6 set for Primary Site, 3 set for Secondary site	
4.0	H3C S5590-28TSXC-EI	**H3C S5590-28TSXC-EI L3 Ethernet Switch, per Switch BoM Including:** - Per Unit BoM Including: H3C S5590-28TSXC-EI L3 Ethernet Switch with 28*10/100/1000 Base-T Ports (Including 4*SFP Combo Ports), 8*1G/10G Base-X SFP Plus Ports and	9

		1*Slot,Without Power Supplies; SFP+ Cable 1.2m; 2 * 180W Asset-Manageable AC Power Supply Module (Power Panel Side Exhaust Airflow); 2 * H3C Fan Module (Fan Panel Side Exhaust Airflow); 5 * Network Product Onsite Service 7×24×4 (5 Yrs MA)	
		UAT#1 & UAT#2 Network Device	
		Internet Zone Firewall - Sangfor Firewall (1 set for UAT#1 & UAT#2)	
5.0		**Reuse Customer's existing 2 X Sangfor AF-1000-FH1600B Firewall in the UAT as Internet Zone Firewall** - Current Sangfor Firewall SNS renewal handled by Customer	1
		Internal Facing firewall - PA (1 x UAT#1 & 1 x UAT#2 internal Zone)	
6.0	PAN-PA-1410	**Palo Alto Networks 1410 (with 5 years Support & Subscription)** - Per Unit BoM including:	2
6.1	PAN-PA-1410	Palo Alto Networks PA-1410	1
6.2	PAN-SVC-BKLN-1410-3YR	PA-1410, Partner enabled premium support	1
6.3	PAN-PA-1410-BND-PRECISIONAI-3YR	PA-1410, Precision AI Network Security Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security, Advanced SD-WAN and Device Security),	1
6.4	PAN-PWR-450W-AC	PA-3400,PA-1400, ION 5200 and ION 9200 450W spare power supply	1
6.5	PAN-1RU-RACK-KIT-4POST	Palo Alto Networks 4-Post rack mount kit for 1U PA-1400	1
6.6	BD-SWAP-PRE	Swapping Service - 24x7x4 (Including On-site Labour)	1
		Network Security Software Tool	
		****EDR Solution**	
7.0	KL40666AQTS	**Kaspersky Next EDR Optimum Hong Kong Edition for 200 x device License EDR, 5 Years** ****Estimated there is 188 servers are requiring the EDR license for protection, and also reserve 12 pcs license for spare	1
		PAM Solution	
8.0		**ManageEngine Privileged Access Manager 360 (PAM360) Enterprise Edition - Subscription Model** Annual subscription fee for 50 administrators and 200 keys, **5 Years License**	1
		SIEM Solution	
9.0		Wazuh / Graylog SIEM - Wazuh / Graylog SIEM for DC1 & DC2 - Wazuh / Graylog SIEM for UAT#1 and UAT#2	1
		Professional Implementation Service for Network And Security	
10.0	PS-IMP	**Profesional Implementation for network & Security config and installation** - Detailed Service Scope please refer to the technical Proposal ******Including the network and Fibre Cable requried for the Project Implementation	1
11.0		**Implementation Service for Implement Wazuh / Graylog SIEM Solution**	1
12		**One- Off Extra Discount Support for Network Setup of the new Environment Setup Project**	1