Terms of Reference

Consultant for the setting up of a National Certification Authority in Sri Lanka

1. Background

With the rapid adoption of commercial ICT-based services by the local populace and the introduction of e-government in the country, it is expected that electronic commerce will grow substantially in the coming years. This also raises the probability of identity theft, financial fraud and other security breaches. To counter this, the ICTA in collaboration with Sri Lanka CERT | CC and other stakeholders has initiated a projected to establish a national framework which defines legal, administrative and technical regulations for granting, managing and enforcing the use of digital certificates to establish the identities of e-services users with the intention of minimizing electronic fraud.

The electronic transactions act no. 19 of 2006 grants authority for a nationally recognized body to perform the function of a National Certification Authority (NCA).

The issue of digital certificates is to be performed through certified third party certificate service providers (CSPs), who are to be licensed by the NCA.

ICTA has already procured hardware,software for the production site of the NCA and in the process of procuring remaining hardware, software for the backup site. As one of the primary objectives of setting up the NCA is to get international recognition, it is mandatory to comply with WebTrust standard.

2. Objective(s) of the Assignment

2.1 To ensure the regulatory and operational framework developed for the NCA is practical, enforceable, widely accepted by the intended user base and aligned with the vision, mission and objectives stated for the NCA.

2.2 To ensure the technological and operational environment of the NCA (production and backup sites) is on a par with other similar initiatives in terms of adopted standards, practices and processes.

2.3 To ensure the confidentiality, integrity, authenticity and reliability of user and root key information and that it is preserved throughout the certification process

2.4 To ensure robust processes and requirements are developed to issue licenses to Certificate Service Providers who are compliant with the licensing requirements and revoking, renewing and auditing such entities.

2.5 To ensure that the specification of hardware and software for the initial build of the NCA (both production and backup site) will sufficient to start the operation of the NCA.

2.6 To ensure that the hardware and software configuration of the NCA (both production and backup site) is done satisfactorily to start the operation of the NCA.

2.7 To ensure that all the documentation requirements are completed to comply with the relevant standards and to start the operation.

3. Scope of Services, Tasks (Components) to be carried out, delivery channels and Expected Deliverables

3.1 Scope of services:

The consultant will be expected to carry out the following services during this consultancy engagement of the NCA. The consultant's expertise will be sought in the areas of system design and planning, regulatory and operational framework development for administration and technology and assisting to document all the required documents to comply with relevant international standards for NCA , such as WebTrust.

3.2 Tasks; Delivery channel; Deliverables

Task is a unique piece of work to be completed during the course of the consultancy engagement. ***Delivery channel*** indicates whether the consultant will be expected to be physically present (on-site) or conduct the work remotely (Remote) from their original location with correspondence occurring via e-mail, online collaboration or teleconferencing. ***Deliverables*** indicate the documentation and any other materials expected by the client at the time of completion of a task.

The following tasks are to be completed by the consultant at times defined within the NCA development roadmap:

3.2.1 Site visit to the location of NCA production and backup site and to meet NCA Task Force and Working Committee to gain background information on completed work; **On-site; Report detailing preliminary findings and recommendations based on site visit.**

3.2.2 Refine and finalize all the developed documents based on latest version of the WebTrust standard and browser/browser forum requirements drafted by the Task Force and Working Committee which is required for the successful operation of the NCA; **Off-site; Finalized documents.**

3.2.3 Assisting the Working Committee to develop the technical and procedural documents based on latest WebTrust, browser forum requirements which are required to start the operation of the NCA and also to comply with the relevant standards. **On-site; Finalized documents.**

3.2.4 Review of the **technological environment** of the NCA with focus on security and functionality; "Recommendations" document. **On-site; Report with recommendations**.

The Technological environment shall consist of:

- The internal communications network including network devices, security devices, cabling,
- External communications facilities such as links, externally hosted services, secure communication channels,
- End devices including servers, clients, security tokens, removable and fixed media and printers
- Physical access control mechanisms including biometric locks, CCTV and environmental technologies including air conditioning, power supply
- Operating OCSP, Web, Directory services

3.2.5 Check and ensure that everything is in order to start the operation of the NCA.This include all the pre-operation testing and key ceremony procedures **On-site; Assistance with recommendations.**

4. Qualification Requirement for the Key Expert (and any other requirements which will be used for evaluating the Expert)

4.1 The consultant should presently be or have been a member of a national security authority which has successfully implemented its own National Certification Authority.

4.2 The key expert must have the following qualifications:

4.2.1 Proven experience in developing the regulatory and operational frameworks for a CA, which has been in successful operation

4.2.2 Demonstrated security knowledge as evidenced by security certifications (CISSP, CISA, etc) or testimonials from past clients detailing work carried out to preserve the confidentiality of information and information security policy development work

5. Final outputs

5.1 For the purpose of the reduced consultancy engagement, deliverables listed in 3.2 shall be submitted in a standard electronic format which can be accessed using a standard software application, where necessary with the use of freely available adaptation software.

Deliverables

No	Deliverables	Payment Milestones
Weeks : 1-2	a. Refine and finalize all the developed documents which is required for the successful operation of the NCA, drafted by the Task Force and Working Committee	20%
Weeks: 3-4	a. Provide recommendations on the current configurations of the NCA production and backup site which include technical and physical environment and controls. b. Assisting the Working Committee to develop the technical and procedural documents which are required to start the operation of the NCA and also to comply with the latest versions of the relevant standards. c. Review of the proposed technological environment of the NCA with focus on security and functionality. d. Check and ensure that everything is in order to start the operation of the NCA.	50%
Weeks: - 5	a. Delivery of any remaining reports	30%