Providing Mauritian PKI Services

Tender No.: ICTA/PKI-1/2004-2005

Issue of Clarification

NOTICE TO ALL TENDERERS

The Authority has decided to amend the implementation schedules as follows:

- ***SECTION A – CLAUSE 2*** *(Tender Forms I,II & III)*
  The successful Tenderer shall commence work within ***TWENTY EIGHT (28) DAYS*** *of receipt of the award of contract and shall proceed to complete and deliver all the work in terms of the express conditions of the contract.*

- ***SECTION B – CLAUSE 28***
  The successful Tenderer shall complete all tasks and requirements laid down in the tender document within ***SIXTEEN (16) WEEKS*** *from the date of award of the contract.*

- ***SECTION C – CLAUSES 12,13 & SCHEDULE III CLAUSE 1(d)***
  HSMs complying to FIPS 140-1 level 3 and above ***will*** *be acceptable.*

(Note: The format of the queries received have been preserved wherever possible)

Queries Set 1

Page Number 15	B. Setting up of two Registration Authorities based in Mauritius to work seamlessly with the Certification Authority outsourced C. Setting up of facilities (hardware & software) for time-stamping at the ICT Authority in Mauritius D. Providing training to the personnel of Registration Authorities for operation and maintenance as well as training for the operation and maintenance of time stamping facilities to the ICT Authority personnel
Based on the above requirements, we need to clarify a few points. Does ICT Mauritius have a data centre of its own where the NTP and the directories can be hosted or will the Tenderer have to procure space and data centre on his own? Where in the world can the Outsourced CA reside? Should they reside in and around Mauritius or can they reside anywhere in the world? Will the Registration Authorities be the responsibility of the Tenderer or only the training and setup portion is involved?	

The ICT Authority requires an independent setup for the housing and operation of time stamping facilities and directories. Space will be made available by the ICT Authority whereas the hardware and software for both of these services will have to be provided by the successful Tenderer

Physical location of outsourced CA may be in any location in the world so long it satisfies **ALL** the conditions spelt out in the Tender document.

The Tenderer bidding for combined RCA, CA & RAs or CA & RAs will be responsible for providing the set up and training for both operation and maintenance of the RAs. Two local agencies will be nominated to be RAs. The provision of staff to operate the RAs will not be the responsibility of the Tenderer as it will be the responsibility of the local agency.

Page 21 Section B.9	Tenderers shall quote fixed Annual recurring charges for the next three years following the date of issue of first certificate. The ICT Authority may, by giving written notice to the Tenderer six (6) months prior to the expiry of the initial period of three years, renew the agreement for another period of three years. The Tenderer shall in such an event continue to make the services offered available on the same terms and conditions except for increase in the annual recurring charges which shall be negotiated between the parties, and which shall in no case exceed 10%.
Required clarifications The recurring cost shall depend upon the facilities to be provided in Mauritius. Will the Tenderer have to setup the data centre, retain Registration Authorities, manpower for network and directories management, etc. Will the Tenderer have to keep up with these costs? Can the upgrade of 10 % be negotiated? As of today it might be difficult to fathom the costs incurred of at that point of time. Can the extension of the next three years be reduced?	

Manpower for time stamping and directory facilities in Mauritius will be provided by ICT Authority.

Manpower for operation of RAs will be provided by the local agencies designated to interface with the outsourced CA. The same RAs (and manpower) will be retained upon renewal of contract.

The increase in recurrent costs upon renewal of contract will be subject to negotiation between parties; **however such increase will in no case exceed 10%.**

Contract renewal will necessarily be for a maximum period of three years upon every renewal.

Page 24 Section B.26	For this tender Public Key Infrastructure (PKI) shall mean hardware, software, cryptographic components, policies, processes and associated personnel.
The extent of PKI in case of this tender is for providing the facilities for the operations part of PKI. In the case as stated in this section, the Tenderer shall have to take care of three components viz. The RCA, the CA and the RA facilities. The policies, processes and the associated personnel shall have to be mutually discussed and decided upon. Based on these conclusions it would be easier to derive the costs.	

All required policies and processes have been spelt out in the schedules I, II, III and IV of the Tender document and should be complied with. As far as training of associated personnel for RAs, time stamping and directories located in Mauritius is concerned, you should quote for the operation and maintenance training in terms of cost/person.

Page 24 Section B.28	Delivery Schedule The successful Tenderer shall complete all tasks and requirements laid down in the tender document within twelve (12) weeks from the date of award of the contract. Any delay shall attract liquidated damages in the amount of US Dollars One Thousand only (US $ 1000/-) per week or part thereof, up to a maximum of 5% of the total contract value.
From the scope of the project, it appears that 12 weeks may be too short a time. Is it possible that more time is given for the completion?	

As per the requests received from several bidders, the successful Tenderer shall complete all tasks and requirements laid down in the tender document within **SIXTEEN (16) WEEKS** from the date of award of the contract.

Page 28	In the proposed model for the Mauritian PKI, outsourcing of RCA and CA operations to a reputed agency is envisaged. Commitment of the Tenderer to operate in strict accordance with the legal and regulatory framework of Mauritius is mandatory.
As we are not familiar with the laws of Mauritius, we would require some time to study and absorb the laws of Mauritius. All the same will ICT Mauritius facilitate in providing the required legal inputs?	

The Mauritius PKI services are subject to various Mauritian laws and jurisdiction of courts, tribunals and authorities in Mauritius. Any specific queries from the successful bidder will be answered at the time of implementation.

Page 28	In addition to hosting of directories by RCA and CA as their normal/regular function, directories hosted by RCA shall also be hosted in Mauritius at the ICT Authority. Time stamping facility shall be provided by CA at its own premises and also at the ICT Authority in Mauritius.
This essentially means we shall have to provide for NTP servers at Mauritius as well as the outsourced location. We need to install directories at both the locations. Does this mean the master directory at the Outsourced location and the shadow directory at ICT Mauritius? The other option is to have two master directories, one at each location and the same directories having a shadow server at each location. Which option has to be followed?	

Tenderers will have to quote for Time Stamping Servers in Mauritius. It is understood that a reputable CA will already have their own time stamping facilities available.

As for the Directories, both the master directory at outsourced CA with shadow in Mauritius as well as two master directories at these locations could be quoted for as two different options. However, the minimum directory requirement in Mauritius is an additional LDAP server at the ICT Authority

Page 32 Section C.28	CA shall update its certificates list and CRLs as soon as possible preferably deploying “Online Certificates Status Protocol" (OCSP).
As it is understood from the statement this is pertaining updating of the CRL. The CRL can be updated at a predefined frequency as well as a forced generation can also be done in case of a revoked certificate. Will the OCSP facility shall be given a preference or will the ON TIME updation of CRL be the core criteria for selection?	

OCSP will be given preference.

Page 33 Section C.32	Security Policy (SP), Certificate Policy (CP) and Certification Practice Statement (CPS) of the Tenderers should conform to relevant International Standards indicated. CP and CPS of RCA and CA will be based on these standards. Selected Tenderer(s) shall provide their assistance and inputs, based on their offered infrastructure and operational experience, to the ICT Authority and licensed CA in finalising SP, CP and CPS of the ICT Authority and the licensed CA. Tenderers shall support unique identification of entities through OIDs.
The documents as described in this point shall be of importance to the ICT Mauritius. Will the Tenderer be required to provide full time consulting for these documents or just assistance to refurbish or reform documents which have already been prepared by the ICT?	

No full time consulting from the vendor will be required. These will be finalised, after discussions, based on the existing policies of the vendor and the requirement of the ICT Authority.

Page 33 Section C.33	The ICT Authority or its authorised representative shall be provided access to reviews, violations and problems as mentioned at subsection 5.1 (i), (j) and (k) of Schedule I on I.T Security guidelines of this section for vendor’s facilities housing RCA and the website. All these logs shall be analysed by the vendor for vulnerability assessment every year. Any shortcomings found shall be attended to. The ICT Authority shall be kept informed.

As earlier declared, we are already hosting the PKI facilities for Indian customers. In this case, the same infrastructure shall be used to support the ICT Mauritius. A certain amount of logs or vulnerabilities, etc shall be common to the ICT Mauritius PKI as well as the PKI for India. Will ICT Mauritius accept the fact the every year an Auditor from Indian for the Indian PKI shall be auditing the logs in its totality? This can also work as an advantage to the ICT Mauritius as the entire setup, starting from physical infrastructure to logical and network security is being audited every year by an empanelled auditor by CCA, India. The ICT Mauritius can save on these costs.

Yes, Mauritius will accept that a reputed auditor approved by the Controller or Authority of the host country carry out the auditing for the RCA facilities and the ICT Authority be kept fully informed of the audit report.

Page 33 Section C.33	In case the ICT Authority decides to revoke the certificate/license of a CA, the RCA shall revoke the PKC and update the CRL within the next 4 (four) working hours after the receipt of authorisation from the ICT Authority.
The working hours of the ICT Mauritius can be different from the RCA as well as the CA for Mauritius as they might be located in different time zones. All the same different countries might be having different holidays, seasons, etc. Based on this a working day in Mauritius can be a holiday in India or vice versa. When ICT Mauritius says 4 working hours, are these working hours as per the Mauritius Time zone?	

The four working hours are those where the outsourced RCA will be located.

Page 49 Section Schedule I 7.a	Security tokens/smart cards/bio-metric technologies such as Iris recognition, finger print verification technologies etc. shall be used to complement the usage of passwords to access the computer system.
Access to data centre is controlled with dual authentication including biometric and cards. Is this required for each and every individual system or only the CA systems as we here consider all the systems in the PKI as sensitive systems?	

Only RCA and CA will need security tokens/smart cards/biometrics technologies to access their computer system.

Page 71 Schedule II 9.1.e	To facilitate decision-making, all agreements and correspondence relating to services provided by Certification Authority should be collected and consolidated, either electronically or manually, at a single location.
As the locations for RCA, CA and RA might be different, the agreements with each vendor, personnel, trusted people, authorised maintenance personnel, etc. have to be located at each place. Can a copy of such agreements be placed at each location?	

Yes, a copy of such agreements can be placed at each location

Page 93 Schedule IV Number 6	In case dual key pair PKI is selected, archiving of encryption Private Key shall be done by the RA for the certificates issued against requests sent by the RA.
The above statement denotes that the ICT Mauritius can also select single key pair technology? Can the Tenderer quote for a single key pair technology with / without encryption?	

Tenderers should be able to support dual key pair PKI system.

Page 94 Schedule IV Number 16	Average down time of the RA facility shall not be more than one hour per month and fault tolerant hardware with necessary redundancy shall be provided.
The downtime of RA can be due to a plethora of reasons, viz. local ISP at any location, manpower problems, electricity, internal network, interconnect between the CA, RCA or the RA as they might be in different countries, etc. Many of these may not be in our control. Does this mean any kind of downtime from the RA shall be calculated?	

The one hour downtime specified includes downtime due to all faults or bugs in the system supplied by the vendor only.

Queries Set 2

1. Please clarify whether the CA services can be hosted under the existing domain (domain name – E.g. www.mauritianpki.tcs-ca.tcs.co.in) of the vendor or should be hosted as a different domain (E.g. www.mauritianpki.mu ? If it has to be hosted as a different domain, then we assume that the vendor will not be responsible for registering and maintaining the domain names. Please clarify whether this assumptions is correct? Otherwise, please clarify whether it is to the option of the vendor.

RCA & CA services will not be hosted on the existing domains of vendors. These have to be hosted as a different domain and the vendor(s) shall be responsible for registering and maintaining the required domains.

2. What should be the storage medium for the Private Key of Time Stamping Authority? Should it be Hardware Security Module (HSM) or Smart Card/ USB Token Soft Certificate (in the system)

Storage medium for the private key of the Time Stamping Authority will be biometric enabled Smart Card/USB token.

3. For the requirement of generating/ storing RCA & CA private keys, HSM of security level FIPS 140-1 level 3 would be highly sufficient. Hence considering the cost effectiveness, we request ICTA to provide an option to the vendor for proposing either level-3 or level-4 HSM.

HSMs complying with FIPS 140-1 level 4 are now available and are preferred over Level 3 compliant HSMs. However HSMs complying to FIPS 140-1 level 3 and above will be acceptable.

4. For the Directory Services requirement RCA and CA, LDAP v3 Directory servers provides the best fit as they are light-weight and tailored for these requirements, as compared to generic X.500 directories which are heavy and complex. Hence, we request ICTA to provide an option to the vendors to propose either X.500 or LDAP v3 directories, which will best suit the requirements.

The Main Directory at vendor's premises must be X500 compliant but the directory hosted at ICT Authority can be LDAP V3 compliant.

5. We request ICTA to clarify whether the country mean Mauritius or the country where the vendor is hosting the RCA/ CA services.

Since the end users certificates are issued only through RA in Mauritius all records as per schedule II section 10 (d) have to be in Mauritius. Therefore the country in clause 10 (d) of schedule II of section C means Mauritius.

6. In *Schedule-III 21) Usage Periods for the Public and Private Keys*, it is specified that the suggested validity period for Certification Authority's root keys, associated certificates and Certification Authority's private signing key is seven years. As these two specifications contradict each-other, we request ICTA to clarify Validity period for RCA key pair and Certificate and Validity period for CA key pairs and Certificates.

Clause 21 of Section C Schedule II indicates the **suggested** validity periods of various keys and certificates. Validity periods of various keys and corresponding certificates **will be** as follows: -

Root Certification Authority	7 years
Certification Authority	5 years
End users (subscribers)	3 years

7. From security perspective, the renewals are suggested to be the creation of new Public Key/ Private Key for the same person/ entity, as the use of existing key-pairs for a prolonged time will result in weakness of the authentication system. As Certificate renewals include creation of new key-pair, it is suggested to be initiated by the certificate holder and approved by the RA. Hence we request ICTA to make this specification as optional and allow for the renewal of the certificates being initiated by the Subscribers.

The subscribers shall initiate such requests and would approach RA. RA only shall generate the request addressed to the CA for renewal of the certificate.

8. We request ICTA to allow the vendor to provide multiple options for costing based on Varied system configurations to suit various performance levels, Varied operating system software/ licensing, and Varied revenue sharing models, etc.

Also provision is required for providing the costing for Digital Certificates issued by CAs. This can be provided as a separate section for the Digital Certificate pricing Digital Certificate pricing to be included in the setup cost. For this, we request ICTA to provide the information of the total number of certificates to be considered for the same.

ICT Authority is not contemplating revenue sharing model with RCA and CA vendors. Vendors may quote for varied system configurations provided each system configuration meets the requirements laid down in the RFP.

9. What is the number of Certificates that will be issued by all the CAs within a period of three years/ Contract period? What will be the total number of CAs under RCA for which the solution has to be proposed? The above details are required for sizing of RCA/ CA infrastructure, Directory server and HSM.

We are expecting 30,000 certificates issued in three years (5K, 10K, 15K) from the date of issue of first certificate. The directory entries expected will be 60,000 in the three years of operation.

Only one CA is planned in the beginning. Provision should be made for two more CAs in the future if the need arises. However for each CA, provision for multiple keys up to a maximum number of five, should be provided in the Root facility.

Queries Set 3

1. Will the 2 RAs that are required to be set up issue certificates under the same CA? If yes, will they be issuing the same type of certificates (are the 2 RA functions identical?)
Two RAs will be issuing the certificates under the same CA. Two RAs will be functionally identical.

2. Is each RA going to be effectively one individual or will there be multiple entities operating under each RA?
Each RA will be an organisation/company. There will not be multiple entities operating under a RA. However important functions within a RA have to be authorised jointly by two persons.

3. Who will decide on the naming of the CA certificates? Who will also decide on the structure and details in the end entity certificates? And when will this be decided?
OID scheme guidelines as per ITU/ISO standards will be given by the ICT authority. The structure and details of the certificates shall be finalised after discussions with the selected CA vendor. The certificate details will be as per relevant international standards.

4. Does ICT also require a full functional Pilot system as well?
There is no reference to "A full functional Pilot System" made in the Tender document issued.

Queries Set 3: Specific queries (with references to specific points in the Tender document)

1. Section B Point 29.e - What exactly requires to be time stamped? Does time stamping here refer to an independent authority signing the transaction time? Which applications will use this service? And how is it intended to work?
The time stamping facility in Mauritius should be able to function on a stand alone basis and should be able to time stamp an electronic transaction, electronic communication and an electronic record. Logs of same will be archived.

Time Stamps in the facility at Mauritius will be signed by persons of the organisation operating the Time Stamp here in Mauritius. The operation of the time stamping facility in Mauritius would be done locally but the responsibility of annual maintenance including providing updates would be of the CA vendor. Vendor shall supply the required H/W and S/W for this facility.

2. Section C Point 3 - What is the objective of having two time stamping facilities? Will they be independent of each other? Who will be responsible for proper functioning of the time server at the ICT authority premises (since this will be out side the secure infrastructure where the rest of the PKI services are hosted)

The time stamping facility in Mauritius should be able to function on a stand alone basis and should be able to time stamp an electronic transaction, electronic communication and an electronic record. Logs of same will be archived.

Time Stamps in the facility at Mauritius will be signed by persons of the organisation operating the Time Stamp here in Mauritius. The operation of the time stamping facility in Mauritius would be done locally but the responsibility of annual maintenance including providing updates would be of the CA vendor. Vendor shall supply the required H/W and S/W for this facility.

3. Section C Point 6 - Is including the ICT root Certificate as a trusted key in browsers within the scope of this tender?

Inclusion of the ICT Authority Root Certificate as a trusted key in browsers is not within the scope of this tender. However the vendor whose infrastructure meets the conditions of section C point 6 would be given preference over vendors whose infrastructure does not meet the specifications.

4. Section C Point 12 - Since most PKI implementations around the world find using HSMs complying to FIPS 140-1 Level 3 adequate, is there any specific reason why FIPS 140-1 Level 4 has been explicitly specified in the Tender? Also, why has an applet been specified for enabling the Root CA installation?

HSMs complying to FIPS 140-1 level 4 are now available and are preferred over Level 3 compliant HSMs. However HSMs complying to FIPS 140-1 level 3 and above will be acceptable.

The applet is required to install the Root Key in the computer system of the relying parties.

5. Section C Point 23 - Is there any specific reason why “cross certificate” is foreseen instead of “cross recognition” especially because cross certification involves other complex issues like unification or normalisation of two different CPSs, building application support to trust cross certificate, etc…

We prefer cross certification and only in cases where it is not possible to cross certify we will allow cross-recognition.

6. Section C Point 25 - Would a signed email be an equally good enough alternative? Also, what is the frequency of the transfer?

All CA certificates issued by the Root and ARL if any, all PKC issued and CRLs of all CAs of the Root are covered under this clause.

Since the Root facility is completely off line the transfer has to be through physical storage devices. The frequency of this would be once a week except when a CA is revoked and in that case it would be immediate and is covered by clause 35 of section **C.**

7. Section C Point 26 - Will this be required to be maintained at the RA end or the CA infrastructure end?
This will be part of CA infrastructure at his end.

8. Section C Point 36 - Please clarify that this point only refers to the usage of the RCA private key and does not include the usage of the CA private key as well.
This point refers to the usage of the RCA private key ONLY.

9. Section C Schedule IV Point 6 - Can we have more details on the key escrow system that is desired? Is the option of a single key pair or dual key pair taken by the certificate applicant? Also, is key escrow optional to the certificate applicant or is it mandatory?
The vendor should be capable of supporting dual key pair PKI. Mauritian PKI will be launched initially as a single key pair PKI. Key escrow system for encryption private keys only is normally a part of dual key pair PKI and therefore Tenderers supporting dual key pair PKI have to describe their key-escrow system.

10. Section C Schedule IV Point 8 - Is the setting up of the smartcard personalisation infrastructure within the scope of this tender as a part of the RA infrastructure?
Yes.

11. Section C Schedule IV Point 15 - Is the capability of issuing 500 certificates per day (8 hours) a requirement of the technical infrastructure (certificate issuance infrastructure) or that of the RA process (physical validation and approval)?
It is the requirement of the technical infrastructure including card personalisation.

12. Section D Point 5 - Will this require only transfer of the private keys only or does the transfer also require the transfer of the certificate issuance application as well?
Requirement is to transfer private keys only. There must be no trace of the private keys left with the vendor after the handing over of the private keys to the ICT Authority.

Queries Set 4

1. What is the tentative amount of certificate ICT is looking for as part of this tender? Evaluation will be done for how many certificates?
We are expecting 30,000 certificates issued in three years (5K, 10K, 15K) from the date of issue of first certificate.

2. How many directory entries license will be needed since this will have cost implication? Evaluation will be done for how many entries?
Directory entries expected will be 60,000 in three years of the operation.

3. What will be the validity of certificates issued? Will ICTA accept certain number of certificate licenses and decide validity as per its policy?
Suggested validity periods of various certificates have been specified under section 21 of schedule II of the RFP. Validity periods of various keys and corresponding certificates **will be** as follows: -

Root Certification Authority	7 years
Certification Authority	5 years
End users (subscribers)	3 years

4. What will be the tender bond value if all the three tender forms are to be filled up. Is full bond value required for individual tender form?
The Tenderers will submit only one tender bond of the amount specified under section F of RFP whether bidding for the full set up or for part of the set up.

5. In Clause 9, instruction to bidder, the time start is calculated from the date of issue of first certificate. Which certificate it is talking about?
For RCA operation the first certificate would be the certificate of CA signed by RCA.
For CA operation the first certificate would be the first PKC of an end user signed by CA.

6. Whether the directory data is required to be stored offline in Mauritius? Also, please clarify whether the ICT wants to house the directory data on LDAP server or requires X.500 compliance. Our Directory is X.500 compliant but the provision of X.500 Directory will further add the cost to the system. Also, what will be the mode of updating of directory data in Mauritius?
The additional directory shall be hosted on a LDAP server at ICT Authority and the contents of which shall be updated by the RCA vendor through secured communication. The annual maintenance including providing updates will be the responsibility of the vendor.

7. What is the purpose of time stamping in ICTA? What kind of services and its provisioning to customer is planned? What will be vendor's responsibility in this?
The time stamping facility in Mauritius should be able to function on a stand alone basis and should be able to time stamp an electronic transaction, electronic communication and an electronic record. Logs of same will be archived.

Time Stamps in the facility at Mauritius will be signed by persons of the organisation operating the Time Stamp here in Mauritius. The operation of the time stamping facility in Mauritius would be done locally but the responsibility of annual maintenance including providing updates would be of the CA vendor. Vendor shall supply the required H/W and S/W for this facility.

8. How many CAs are required to be created?
Only one CA will be created in the beginning. Provision should be made for two more CAs in the future if the need arises. However for each CA, provision for multiple keys up to a maximum number of five, should be provided in the Root facility.

9. Are the CA and RCA private key required to be on the different token or it can reside on the same token?
Yes the private keys of both RCA and CA can reside on the same HSM.

10. It may please be clarified whether FIPS 104-1 Level 3 compliant HSM and Token will be acceptable? CCA India accepts FIPS 104-1 level 3.
HSMs complying with FIPS 140-1 level 4 are now available and are preferred over Level 3 compliant HSMs. However HSMs complying to FIPS 140-1 level 3 and above will be acceptable.

11. Who will issue the OID?
OID scheme guidelines as per ITU/ISO standards will be given by the ICT authority. The structure and details of the certificates shall be finalised after discussions with the selected vendor(s). The certificate details will be as per relevant international standards.

12. Will ICTA prefer to provide its own site in Mauritius or wants the vendor to provide space and environment (AC, UPS, etc.)? In that case, what will be the time period used for evaluation and the commitment period? It is understood that the vendor will provide all surveillance and monitoring devices. Please confirm.
For Directory Services and Time Stamping facilities in Mauritius the space will be made available by the ICT Authority whereas the hardware and software for both of these services will have to be provided by the successful Tenderer. For RAs the site will be provided by the designated local agency but providing the entire infrastructure (the hardware and software) will be the responsibility of CA vendor.

13. How much secure site is needed for Directory physical infrastructure?
Normal security is required as there is no signing involved in Mauritius and the signed directory data would be coming from the vendor.

14. How far the two RAs will be located? Can one RA and Directory physical site be co-located? How much secure site is needed for RA physical infrastructure?
Two RAs will be at different locations in Mauritius. Normal security only is to be provided for RA installations. Directory shall not be co located with RA.

15. Will ICTA accept Audit of infrastructure by CCA India?
ICT Authority will accept the audit of the infrastructure by any of the auditor approved by Controller or (Authority) of the host (vendor's) country. Copy of the relevant Audit Report has to be supplied to ICT Authority.

16. What will be the frequency of audit (internal by vendor and external by ICTA or ICTA appointed agency)? What will be cost apportioning for such activity?
Frequency of Audit will be as prescribed by Controller or Authority of the country where vendor has the infrastructure. All costs of all audits shall be borne by the vendor. Audit performed by local authority will be accepted by ICTA and the audit reports of such audits have to be submitted to ICT Authority.

17. Is there any plan to issue the certificate from web site? If so, please provide details.
No plans to issue certificates from the web site.

18. Please convey the details regarding the billing package if required?
A Standard billing package as per international best practices is acceptable.

19. What will be the mode of operations of CA business? What classes of certificates are planned? Projection, year wise, may also be conveyed.
It is planned to issue three classes of certificates in the beginning but the facility should exist to have more classes in the future.

20. The start date of the project is mentioned as 7 days from contact. This is too short. We recommend minimum of 4 weeks since there will be a lead time to deliver the equipments and services to Mauritius.
As per the requests received from several bidders, the successful Tenderer shall commence work within **TWENTY EIGHT (28) DAYS** of receipt of the award of

contract and shall proceed to complete and deliver all the work in terms of the express conditions of the contract.

21. The project delivery of 12 weeks is too short. In our experience this should not include time for audit and certification etc.

As per the requests received from several bidders, the successful Tenderer shall complete all tasks and requirements laid down in the tender document within **SIXTEEN (16) WEEKS** from the date of award of the contract.

Queries Set 5

Option 1) Registration Authorities only

Based in Mauritius with Root CA and CA services based elsewhere, questions are as follows:

1) What technology will be used (VeriSign or RSA recommended due to all preliminary work done in CPS, CP, contracts, user-friendly interfaces, recognized in over 300 standard applications)?

Technology used will depend on the vendor selected.

2) Who will be the partner that will host the Root and CA services?

Depends on selected vendor.

3) Should the physical and logical security need to be planned?

Refer to schedules I, II , III and IV of Tender Document.

Option 2) Complete Trust Centre

Based in Mauritius and operating as an independent entity, our questions are as follows:

1) What technology will be used, VeriSign or RSA preferred due to the following:

a. Already existing CP, CPS, contracts,

b. Security clearance procedures,

c. segregation of duties documents

d. Operational procedures

e. Authentication processes

f. Application integration?

2) Who will be the solution partner?

3) The only discrepancy is that in the tender it states that the project needs to be completed within a 3 month period. Planning and installation of 2 Registration Authorities in that timeframe is possible but designing and building a complete Trust Centre can take anything up to 1 year. Kindly advise on possibility of reviewing the timeframe.

As per the Tender Document no Trust Centre (RCA and CA) is mandatory in Mauritius.

Other Queries

Please advise on the number and the maximum capacity of printing machines for Smartcards.

500 Smart Cards per day

· Is time stamping in Mauritius required?

Yes it is required

· Does ICTA require Key Management and recovery?

Please refer to Section C of the Tender Document

· Does ICTA require Directory Services technology?

Hosting of directory at the ICT Authority will be the responsibility of the selected vendor.

· Does ICTA require Website development?

No

· Does ICTA require Disaster recovery site?

Please refer to Section C of the Tender Document – this will be the responsibility of the selected vendor

· Please advise on Cross Certification (to what CAs)?

Please refer to Section C of the Tender Document – Provision exists for cross certification with other CAs

· Please advise how many certificates ICTA plan to issue (Year 1, Year 2 & Year 3)

We are expecting 30,000 certificates issued in three years (5K, 10K, 15K) from the date of issue of first certificate.

· What is the Percentage of soft certificates versus smartcard certificates?

This will be known after operation starts with selected vendor since this depends on several factors.

· What certificate types is ICTA planning to issue (VPN, SSL, SMIME etc)?

It is planned to issue three classes of certificates in the beginning but the facility should exist to have more classes in the future.

· Has the ICTA already selected a secure physical site

The secured physical site for RCA and CA will be located at vendor's site.

Queries Set 6

1) Can you elaborate on the decision making criteria in terms of your vendor, system integrator (SI) and hosting strategies, for example would you favour a solution where a single vendor can provide all the elements or do you envisage a situation where you might choose a technology from one submission and a SI from another bid and so on.
The best solution will be the most cost effective one which meets **all** the technical requirements laid down in the Tender document and which will be deployed in the set time frame.

2) What is the most important aspect of your decision, price, capability, commitment to a go live date and accomplishment of the project within that deadline, best of breed technology etc.
The best solution will be the most cost effective one which meets all the technical requirements laid down in the Tender document and which will be deployed in the set time frame.

3) Can you clarify the exact numbers? The RFP suggests a user community of 500 USB Tokens and 200 smart cards and readers. Can you state what the next phase will be and for what purpose.
We are expecting 30,000 certificates issued in three years (5K, 10K, 15K) from the date of issue of first certificate.

4) Please can you describe, who will user the USB Tokens and what applications do they need to authenticate to and who are the smart card users?
USB tokens and Smart Cards are functionally identical and both may be used in for the same application

5) Will any of the above users need to utilise they're certificate on a smart card or token for digitally signing? Please can you describe what applications these users would be signing and the workflow around that.
PKCs on Smart Cards or USB tokens are mainly used for digital signatures.

6) From page 27, paragraph 21. Certificate life cycle management for the user certificates shall be done by the licensed CA through RAs in Mauritius.
Q: Would a solution which automated user key and certificate lifecycle management be acceptable. Specifically, user key and certificate update could be automated, without requiring any RA or user involvement. This would obviously reduce the cost of the system, and improve the user experience by not requiring the user to reregister if they are already trusted by the CA.

The RCA and CA can be outside Mauritius and therefore certificates management is performed by RAs only.

7) From page 28, paragraph 25. Signed certificates and signed directories (both certificates and CRLs) shall be transferred from the offline signing system to the RCA website physically through storage media devices like CDs, pen drives, etc. These media devices shall be marked and archived.
Q: What is meant by "signed directories"? Does this mean that all of the sensitive information within the directories (including certificates and CRLs) are individually signed?
Relevant directories will be signed by the issuers (RCA or CAs) as per international standards.

8) From page 28, paragraph 30. All certificates issued to CAs, repository of all certificates and CRLs shall be displayed, as per standards, on the website.
Q: Given that user certificates will be in the X.500 repository (paragraph 31), what standards should be followed in publishing certificates to the Web site?
ITU X.509 standards will be followed.

9) From page 21, the terms of payment is 90% for the one time fixed charges on the issue of first PKC and the availability of all directories on the website.
Q: Can the project be broken in phases by the ICTA and payment made upon the successful completion of each phase? Alternatively, can a half-payment of the 90% one time fixed charges be made upon the issue of the first PKC?
Payment schedules are as laid down in the Tender document.

Queries Set 7

RFP document related:

"Setting up secured facilities for hosting of directories and setting up facilities for time stamping services": does it include firewalls, IDS, monitoring system, routers, cabling, power supply, backup power supply, etc.

Is it possible to give a more detailed description of the deliverable.

Please refer to Sections B and C of the Tender document.

Page 25 §4 "The operation of RCA and CA shall be governed by the legal and regulatory framework of Mauritius": where can we find more information about this?

The Mauritius PKI services are subject to various Mauritian laws and jurisdiction of courts, tribunals and authorities in Mauritius. Any specific queries from the successful bidder will be answered at the time of implementation.

Page 26 §12 + §13 are defining that FIPS 140-1 level 4 is required, while page 26 §16 and page 27 §17 is defining that a back-up of the private key is required. As far as we know, FIPS 140-1 level 4 (specifications designed for unattended security system within a non secure environment, e.g. payment terminals) does not allow to export the private key in any form. While FIPS 140-1 level 3 is fully supporting the mechanism as defined within §18.3 a) page 72. Could it be that there is mismatch with the definition of the requirements?

HSMs complying with FIPS 140-1 level 4 are now available and are preferred over Level 3 compliant HSMs. However HSMs complying to FIPS 140-1 level 3 and above will be acceptable.

Page 27 §19 "... who shall request CA on internet/VPN in safe and secure way ...": Are alternatives like SSL sessions with client authentication acceptable?

The RAs

Page 29 §32 "Tenderers shall support unique identification of entities through OIDs": Can this be clarified (e.g. is this referring to the usage of OID within a certificate to identify policies)? Who owns the OID's ICTA or the successful tenderer?

OID scheme guidelines as per ITU/ISO standards will be given by the ICT authority.

General questions:

How many licensed CAs needs to be supported?

Only one CA will be created in the beginning. Provision should be made for two more CAs in the future if the need arises

What is the expected volume of end-entity certificates to be issued per year?
We are expecting 30,000 certificates issued in three years (5K, 10K, 15K) from the date of issue of first certificate.

What are the requirement related to scalability (see above: support for multiple CA's and RA's)?
Only one CA will be created in the beginning. Provision should be made for two more CAs in the future if the need arises.

Pricing - How to indicate variants / options / additional services (e.g. OCSP services, etc.) within the prices tables? Do we need to the use the templates included within the RFP or can we define our own price table?
Are functional and technical specifications available or is the definition of these specifications part of the project / deliverables?
Please refer to the Tender document especially section D of the Tender document. Options and additional services details may be attached as annex.