ICTA

PROVIDING MAURITIAN PKI SERVICES

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

Request for Proposal

IMPORTANT DATES

•	*Date of issue of Tender (RFP)*	-	*11th August 2004*
•	*Last date for reception of queries from Tenderers*	-	*1st September 2004*
•	*Issue of clarification (if any) by ICT Authority*	-	*6th September 2004*
•	*Closing date of Tender*	-	*20th September 2004*

INFORMATION & COMMUNICATION TECHNOLOGIES AUTHORITY

Request for Proposal

1st Floor Jade House • Cnr. Jummah Mosque & Remy Ollier Streets • Port Louis • Mauritius
Phone (230) 217 2222 • Fax: (230) 217 7777
Email: icta@intnet.mu • Web: www.icta.mu

INFORMATION & COMMUNICATION
TECHNOLOGIES AUTHORITY

Table of Contents

Section

A

A. FORMS OF TENDER

- *Tender Form I – Bid for RCA, CA and RAs*
- *Tender Form II – Bid for RCA*
- *Tender Form III – Bid for CA and RAs*

ICT AUTHORITY

(Tender Form I)

FORM OF TENDER – ROOT CERTIFICATION AUTHORITY (RCA), CERTIFICATION AUTHORITY (CA) AND TWO REGISTRATION AUTHORITIES (RAs)

(To be filled by Tenderers bidding for **combined** RCA, CA and RAs)

TENDER NO.: ICTA/PKI-1/2004-2005

This Tender Form issued to .... must be delivered, duly completed and addressed to the Executive Director, ICT Authority, Port Louis and should be deposited in the Tender Box, ICT Authority, 1st Floor, Jade House, cnr Jummah Mosque & Remy Ollier Streets, Port Louis at latest by 14.00 hrs. on 20th September 2004.

Tenders received after the specified time and date will not be considered.

The ICT Authority reserves the right to accept or reject any Tender and to annul the tendering process and reject all Tenders at any time prior to award of contract without thereby incurring any liability to Tenderers or any obligation to inform the Tenderers of the grounds for the ICT Authority's action.

....

Persons tendering are required to fill in all the blank spaces in this Tender Form.

To:

The Executive Director,

ICT Authority

Sir,

Having examined all the documents making up the Table of Contents including the financial proposal as per the Financial Summary Sheet for the setting-up, commissioning and maintenance of the following turn-key works: -

Setting up of the Public Key Infrastructure (PKI) for Mauritius by:

A. **Providing the Root Certification Authority facilities/services including hosting of directories on its secured website on behalf of the ICT Authority**

B. **Providing the Certification Authority (CA) facilities/services including hosting of directories on its secured website on behalf of the CA to be licensed by the ICT Authority**

C. **Setting up two Registration Authorities based in Mauritius to operate seamlessly with the designated Certification Authority**

D. **Setting up secured facilities (including hardware & software) for hosting of directories at the ICT Authority**

E. **Setting up facilities (including hardware & software) for time-stamping services at the ICT Authority**

F. **Providing operation and maintenance training for designated personnel for the Registration Authority/Authorities, directory and time-stamping services**

1. We agree to execute and provide all the functions and services therein referred to, in full conformity with the tender documents and to your entire satisfaction .Our charges shall

be as follows: -

Functions	**One time charge** **(US Dollars)**	**Annual recurring charges** **(US Dollars)**
Root Certification Authority including hosting of directories on its secured website and Certification Authority (CA) including hosting of directories on its secured website		
Setting up of Two Registration Authorities in Mauritius		
Setting up of secured facilities (hardware & software) for hosting of directories at the ICT Authority		
Setting up of facilities (hardware & software) for time-stamping at the ICT Authority in Mauritius		
Operation & Maintenance Training of personnel of RAs (Total Cost)		Not Applicable
Operation & Maintenance Training for directory hosting for personnel of the ICT Authority (Total Cost)		Not Applicable
Operation & Maintenance Training for time stamping for personnel of the ICT Authority (Total Cost)		Not Applicable

2. We further undertake, upon acceptance of our tender, to commence work within 7 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.

3. We undertake to furnish a Performance Bond as required within 7 days from the date of acceptance of the tender and sign the contract when convened to do so.

4. We herewith attach a security in the form of a Tender Bond from (……………………………………………………………………………………), a Bank established in Mauritius, in the sum of Mauritian Rupees One Hundred and Fifty Thousands only *(Rs 150,000/-)* and we agree that this sum shall be forfeited in the event we refuse to execute the contract after your formal acceptance of our tender.

Note: TENDER BOND TO BE SUBMITTED IN ORIGINAL. TENDER BOND SUBMITTED BY FAX IS NOT ACCEPTABLE. A BANKER'S OFFICE CHEQUE IS ACCEPTABLE.

5. Unless and until a formal Agreement has been prepared and executed, this Tender, together with your written acceptance thereof, shall constitute a binding Contract between us and the ICT Authority.

TENDERER ………………………	WITNESS………………............................
(SIGNATURE)	(SIGNATURE)
NAME..................... …………………	NAME...............………………………….
ADDRESS	ADDRESS…..
…………………………………………	………………..
DATE……………………………………	DATE……………………………………….
PHONE NO.: ……………………………	PHONE NO.: ………………………………
EMAIL…………………………………..	EMAIL……………………………………....

ICT AUTHORITY

(Tender Form II)

FORM OF TENDER – ROOT CERTIFICATION AUTHORITY (RCA)

(To be filled by Tenderers bidding **only** for RCA)

TENDER NO.: ICTA/PKI-1/2004-2005

This Tender Form issued to .... must be delivered, duly completed and addressed to the Executive Director, ICT Authority, Port Louis and should be deposited in the Tender Box, ICT Authority, 1st Floor, Jade House, cnr Jummah Mosque & Remy Ollier Streets, Port Louis at latest by 14.00 hrs. on 20th September 2004.

Tenders received after the specified time and date will not be considered.

The ICT Authority reserves the right to accept or reject any Tender and to annul the tendering process and reject all Tenders at any time prior to award of contract without thereby incurring any liability to Tenderers or any obligation to inform the Tenderers of the grounds for the ICT Authority's action.

....

Persons tendering are required to fill in all the blank spaces in this Tender Form.

To:

The Executive Director,

ICT Authority

Sir,

Having examined all the documents making up the Table of Contents including the financial proposal as per the Financial Summary Sheet for the setting-up, commissioning and maintenance of the following turn-key works: -

Providing the Public Key Infrastructure (PKI) for Mauritius:

A. **Outsourcing of the Root Certification Authority including hosting of directories on its secured website on behalf of the ICT Authority**
B. **Setting up of secured facilities (hardware & software) for hosting of directories at the ICT Authority**
C. **Providing training for the personnel of the ICT Authority**

1 We agree to execute and provide all the functions and services therein referred to, in full conformity with the tender documents and to your entire satisfaction .Our charges shall be as follows: -

Functions	One time charge (US Dollars)	Annual recurring charges (US Dollars)
Root Certification Authority (RCA) including hosting of directories at its website		
Setting up of facilities for hosting of directories at the ICT Authority in Mauritius		
Operation & Maintenance Training for directory hosting for personnel of the ICT Authority (Total Cost)		Not Applicable

2. We further undertake, upon acceptance of our tender, to commence work within 7 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.

3. We undertake to furnish a Performance Bond as required within 7 days from the date of acceptance of the tender and sign the contract when convened to do so.

4. We herewith attach a security in the form of a Tender Bond from (……………………………………………………………………………………………), a Bank established in Mauritius in the sum Mauritian Rupees One Hundred and Fifty Thousands only *(Rs 150,000/-)* and we agree that this sum shall be forfeited in the event we refuse to execute the contract after your formal acceptance of our tender.

Note: TENDER BOND TO BE SUBMITTED IN ORIGINAL. TENDER BOND SUBMITTED BY FAX IS NOT ACCEPTABLE. A BANKER'S OFFICE CHEQUE IS ACCEPTABLE.

5. Unless and until a formal Agreement has been prepared and executed, this Tender, together with your written acceptance thereof, shall constitute a binding Contract between us and the ICT Authority.

TENDERER ………………………	WITNESS…………………..............................
(SIGNATURE)	(SIGNATURE)
NAME...................... …………………	NAME...............…………………………….
ADDRESS	ADDRESS…...
…………………………………………	…………………..
DATE……………………………………	DATE……………………………………….
PHONE NO.: ……………………………	PHONE NO.: ………………………………
EMAIL…………………………………..	EMAIL……………………………………...

ICT AUTHORITY

(Tender Form III)

FORM OF TENDER – CERTIFICATION AUTHORITY (CA) AND TWO REGISTRATION AUTHORITIES (RAs)

(To be filled by Tenderers bidding **only** for CA and RAs)

TENDER NO.: ICTA/PKI-1/2004-2005

This Tender Form issued to .... must be delivered, duly completed and addressed to the Executive Director, ICT Authority, Port Louis and should be deposited in the Tender Box, ICT Authority, 1st Floor, Jade House, cnr Jummah Mosque & Remy Ollier Streets, Port Louis at latest by 14.00 hrs. on 20th September 2004.

Tenders received after the specified time and date will not be considered.

The ICT Authority reserves the right to accept or reject any Tender and to annul the tendering process and reject all Tenders at any time prior to award of contract without thereby incurring any liability to Tenderers or any obligation to inform the Tenderers of the grounds for the ICT Authority's action.

....

Persons tendering are required to fill in all the blank spaces in this Tender Form.

To:

The Executive Director,

ICT Authority

Sir,

Having examined all the documents making up the Table of Contents including the financial proposal as per the Financial Summary Sheet for the setting-up, commissioning and maintenance of the following turn-key works: -

Providing the Public Key Infrastructure (PKI) for Mauritius:

A. **Outsourcing the Certification Authority of Mauritius on behalf of the CA to be licensed by the ICT Authority**

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**

1. We agree to execute and provide all the functions and services therein referred to, in full conformity with the tender documents and to your entire satisfaction. Our charges shall be as follows: -

Functions	**One time charges** **(US Dollars)**	**Annual recurring charges** **(US Dollars)**
Certification Authority (CA) including hosting of directories on its secured website		
Setting up of Two Registration Authorities in Mauritius		
Setting up of facilities (hardware & software) for time-stamping at the ICT Authority in Mauritius		
Operation & Maintenance Training for personnel of RAs (Total Cost)		Not Applicable
Operation & Maintenance Training for time stamping for personnel of the ICT Authority (Total Cost)		Not Applicable

2. We further undertake, upon acceptance of our tender, to commence work within 7 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.

3. We undertake to furnish a Performance Bond as required within 7 days from the date of acceptance of the tender and sign the contract when convened to do so.

4. We herewith attach a security in the form of a Tender Bond from (……………………………………………………………………………………), a Bank established in Mauritius in the sum Mauritian Rupees One Hundred and Fifty

Thousands only *(Rs 150,000/-)* and we agree that this sum shall be forfeited in the event we refuse to execute the contract after your formal acceptance of our tender.

Note: TENDER BOND TO BE SUBMITTED IN ORIGINAL. TENDER BOND SUBMITTED BY FAX IS NOT ACCEPTABLE. A BANKER'S OFFICE CHEQUE IS ACCEPTABLE.

5. Unless and until a formal Agreement has been prepared and executed, this Tender, together with your written acceptance thereof, shall constitute a binding Contract between us and the ICT Authority.

TENDERER ………………………	WITNESS………………..............................
(SIGNATURE)	(SIGNATURE)
NAME..................... …………………	NAME...............……………………………
ADDRESS	ADDRESS…...
…………………………………………	………………..
DATE……………………………………	DATE……………………………………….
PHONE NO.: ……………………………	PHONE NO.: ………………………………
EMAIL…………………………………..	EMAIL……………………………………....

Section

B

B. INSTRUCTIONS TO TENDERERS

ICT AUTHORITY

INSTRUCTIONS TO TENDERERS

TENDER NO.: ICTA/PKI-1/2004-2005

In pursuance of the Information and Communication Technologies Act 2001 as amended, the ICT Authority proposes to establish the Mauritian Public Key Infrastructure (PKI) to create a secure environment for e-commerce and e-governance applications in Mauritius. Cost, quality and time to start services shall be essential considerations. The Root Certification Authority (RCA) operation and Certification Authority (CA) operation would be outsourced to experienced and reputed vendor(s) with required infrastructure and processes in place. PKI providers and CAs are invited to tender for the following works in accordance with the instructions set forth below: -

1. Tenders are being invited for the outsourcing of RCA and CA including the setting up of two Registration Authorities (RAs) in Mauritius for accepting applications/requests from users and delivery of certificates to them.

2. The Tender Documents shall consist of: -

(a) Forms of Tender

(b) Instructions to Tenderers

(c) Specifications /Technical requirements

(i) Information Technology Security Guidelines Schedule I

(ii) Security Guidelines for Certification Authorities Schedule II

(iii) Standards followed by Certification Authorities Schedule III

(iv) Requirements for Registration Authority (RA) Schedule IV

(d) Conditions as required by the ICT Authority

(e) Financial Summary Sheets

(f) Form of Tender Bond

(g) Form of Agreement

(h) Form of Performance Bond

3. (a) Tenderers shall fill in all the three tender forms (Form I, Form II and Form III) and all the corresponding Financial Summary sheets when bidding for RCA, CA and two RAs services/facilities.

(b) Tenderers bidding only for RCA services/facilities shall fill in Form 2 only along with the corresponding Financial Summary sheet.

(c) Tenderers bidding only for CA and two RAs services/facilities shall fill in form 3 only along with the corresponding Financial Summary sheet.

4. The Tenderers shall check all documents for completeness against the table of contents and shall check all pages of the Tender Documents. Should the Tenderer find any page missing/in duplicate or any figures and the corresponding wording indistinct, or be in doubt as to the true meaning of any part of the Tender Documents, he shall at once notify the:

EXECUTIVE DIRECTOR
ICT AUTHORITY
PORT LOUIS

,and in any case not later than 20 days prior to the date set for the closing of the tenders. Any clarification or amendment will be issued formally by final addenda to all Tenderers. All discrepancies shall thereupon be rectified by the Tenderer. Addenda revising, adding to or deducting from the Tender Documents may be issued by the Executive Director, ICT Authority either in response to the request from prospective Tenderers for explanations or for other reasons. Each addendum will be issued to all Tenderers who have been issued with the tender documents. Such addendum will become part of the Contract Documents and receipt thereof must be acknowledged immediately by signing and returning the acknowledgement form distributed with the addendum.

No liability will be admitted nor any claim allowed in respect of errors, mistakes or discrepancies in the submission of Tender Documents to the tenders which should have been rectified in the manner described above.

5. The Tender Documents may be obtained from the Executive Director, ICT Authority.

6. All Tender Documents and correspondence shall be drawn up in English only.

Tenderers shall complete the Form of Tender(s), Form of Tender Bond, Financial Summary

Sheet(s) and all the attachments required. Offer shall be submitted in two sealed covers. The first sealed cover shall be duly labelled **"PRICE PROPOSAL"** and shall contain the financial sections (Form(s) of Tender and Financial Summary Sheet(s)) of the bid. The second sealed cover shall contain the rest of the bid including the Tender Bond and shall be duly labelled **"TECHNICAL AND COMMERCIAL PROPOSAL"**. Both sealed covers shall be placed in a third sealed cover duly labelled **"BID AGAINST TENDER NO.: ICTA/PKI-1/2004-2005"** and addressed to:

EXECUTIVE DIRECTOR
ICT AUTHORITY,
1st Floor, Jade House,
cnr. Jummah Mosque & Remy Ollier Streets,
PORT LOUIS.
MAURITIUS.

,and shall be deposited in the Tender Box situated at the same address at latest by **14.00 hours on Monday, 20th September 2004.**

N.B. TENDERS AND TENDER BOND SUBMITTED BY FAX WILL NOT BE ACCEPTED

7. Tenderers may quote only for RCA or only for CA including RAs or for both RCA and CA including RAs. They should clearly indicate the break up of costs for each facility. The ICT Authority shall have full authority to award the contract for only RCA or for only CA including RAs or for both RCA and CA including RAs.

8. Tenderers are required to submit their tender on a one time fixed charge and on annual recurring charges basis for executing all the work, facilities and services referred to in the tender documents.

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%.

10. In order to secure the due performance by Bidders of the obligations undertaken by them, a Security in the form of an original Tender Bond from a local bank in the sum of Mauritian Rupees One Hundred and Fifty Thousands only *(Rs 150,000/-)* is required to be submitted with the tender.

(a) The amount of the Tender Bond shall be forfeited to the ICT Authority in the event the Tenderer withdraws his Tender or part thereof before expiration of its validity period including any extension agreed upon with the Tenderer and/or fails to enter into contract, and submit a Performance Bond, within seven (7) days after an award is made to him by the Executive Director, ICT Authority.

The Tender Bond shall be valid for one hundred and eighty (180) days from the date of closing of the tender.

(b) The security provided by unsuccessful Tenderers shall be repaid or discharged only after finalisation of the tender and the acceptance by the successful Tenderer and submission of the performance bond.

(c) The security provided by the Tenderer whose tender is accepted shall be repaid or discharged when the Performance Bond has been duly entered into and executed.

11. Tenderers shall submit all details as required in Section D of the tender document.

12. The bid (Form of Tender duly filled and other documents including the Financial Summary Sheets) submitted must be completed in every respect.

13. Any conditional bid will be rejected.

14. Incomplete bids will not be considered.

15. An identical soft copy of the complete response/bid shall be provided in addition to the duly signed hard copy.

16. The ICT Authority shall not be liable in respect of any expenses or losses which may be incurred by a Tenderer in the preparation and submission of the Tenders.

17. The successful Tenderer will also be required to provide a bank guarantee for the good performance of the contract (Performance Bond) in an amount equivalent to 10% of the Contract Price including annual recurring charges. **The Performance Bond should be valid for thirty six (36) months.**

18. The tender shall be governed by the laws applicable in Mauritius.

19. All activities arising from the tender shall be completed within the time schedule prescribed. In default Liquidated and Ascertained damages shall be levied.

20. The Tenderer shall ensure that his Tender is arithmetically correct in all respects. All amounts should be expressed in words and in figures.

21. The Tenderer shall clearly indicate all points/cases where his bid is **not** in conformity to the specifications/requirements laid down in the tender document.

22. Notification of Award of Contract shall be made by the Executive Director, ICT Authority.

23. The ICT Authority reserves the right to split, accept or reject any tender and to annul the tendering process and reject all Tenders at any time prior to award of contract without thereby incurring any liability to any Tenderer or any obligation to inform the Tenderer of the grounds for the ICT Authority's action. The ICT Authority also reserves the right to order/commission selective components.

24. Until a formal agreement has been prepared and executed, the tender(s) together with the written acceptance of the ICT Authority shall constitute a binding contract between the ICT Authority and the Tenderer.

25. The apparent silence of this specification and any supplemental specifications as to any details or the omission from it of a detailed description concerning any point shall be regarded as meaning that only the best commercial/professional practices meeting international standards are to prevail and that only top quality services are to be provided. All interpretations of the specifications shall be made upon the basis of this statement.

26. For this tender Public Key Infrastructure (PKI) shall mean hardware, software, cryptographic components, policies, processes and associated personnel.

27. The tender must be signed by the person duly authorised to do so. A Tender submitted by a company must bear the seal of the company duly attested by the Company Secretary. A Tender submitted by a joint venture of two or more firms must be accompanied by the authentic deed witnessing such joint-venture or a certified true Photostat copy thereof.

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.

29. **Acceptance Testing Procedure**

a) RCA and its website hosting directories/Certificate Revocation List (CRL)

Representative(s) of the ICT Authority will visit the facilities of the successful Tenderer to verify the conformity of the infrastructure, processes, facilities and services to the specifications and requirements laid down in the tender document. A date for key generation shall then be fixed for generating the key pair in the HSM and issuing a self signed RCA certificate. This certificate shall then be displayed on the website of the RCA for distribution to all relying parties.

b) CA and its website hosting directories/CRL

Representative(s) of the ICT Authority will visit the facilities of the successful Tenderer to verify the conformity of the infrastructure, processes, facilities and services to the specifications and requirements laid down in the tender document. A date for the key generation shall then be fixed for generating the key pair in the HSM. The public key of this key pair shall then be submitted to the RCA for signature by the Root Key. The CA certificate will then be displayed on the CA website for distribution to all relying parties.

c) Setting up two RAs in Mauritius

After installation of the RA facilities by the successful Tenderer, the representative(s) of the ICT Authority shall verify the conformity of the infrastructure installed, processes, facilities and services to the specifications and requirements laid down in the tender document. Trial key pairs will be generated on smart-cards as well as on I-keys and requests shall be made to CA for issuing trial certificates. Some trial certificates shall similarly be revoked as part of the trial. Printing on smart-cards shall also be checked for error free printing.

d) Setting up directory facilities in Mauritius

Representative(s) of the ICT Authority will verify the conformity of the infrastructure installed, processes, facilities and services to the specifications and requirements laid down in the tender document. Directories and access procedures shall be tested by creating entries for the trial certificates.

e) Setting up of time-stamping facilities in Mauritius

Representative(s) of the ICT Authority will verify the adequacy of the infrastructure and archiving and will send messages on the Internet to verify that these messages are correctly time-stamped and properly archived by the time stamping facility in Mauritius.

30. Terms of Payment:

a) 90% of the one time fixed charges on the issue of first Public Key Certificate (PKC) and the availability of all directories on the web site.

b) 25% of annual recurring charges after every three months of providing satisfactory services.

c) **The remaining 10% of the fixed** charges shall constitute a retainer that will be disbursed one year after the date of issue of first PKC upon successful provision of services. However, this amount may be released against the submission of a bank guarantee for an equivalent amount valid for one year.

I/We the undersigned have read and understood the instructions to Tenderers set out at paragraphs 1 to 30 above and acknowledge the same.

TENDERER:…...……………………………………….

SIGNATURE:………………………………………..

NAME:…………..

DESIGNATION:.……………………………………….

DATE:…………………………………………………..

Section

C

C. SPECIFICATIONS

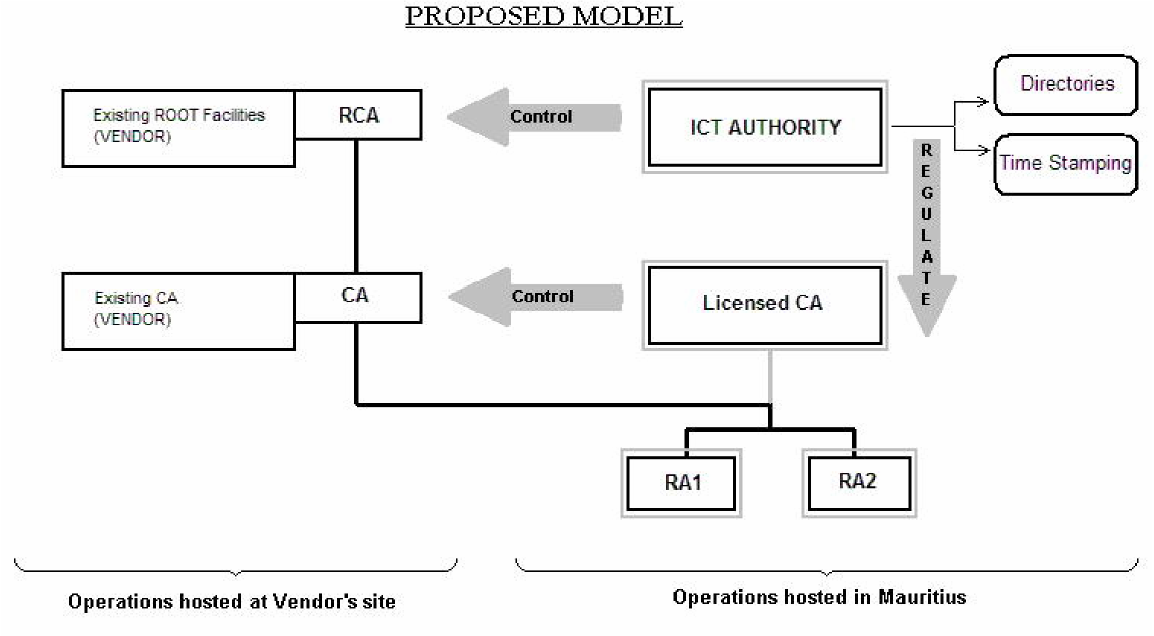
- *Schedule I - Information Technology Security Guidelines*
- *Schedule II - Security Guidelines for Certification Authorities*
- *Schedule III - The standards followed by Certification Authority*
- *Schedule IV - Requirements For Registration Authority*

ICT AUTHORITY

SPECIFICATIONS

TENDER NO.: ICTA/PKI-1/2004-2005

1. In pursuance of the Information and Communication Technologies Act 2001 as amended, the ICT Authority proposes to establish the Mauritian Public Key Infrastructure (PKI) to create a secure environment for e-commerce and e-governance applications in Mauritius.
2. The ICT Authority will be the "Root Certification Authority" (RCA). An appropriate agency would be licensed to become the first Certification Authority i.e. the **Licensed CA** of Mauritius. The RCA and CA operations are to be outsourced to experienced and reputed vendor(s) with adequate existing infrastructure and processes.
3. The proposed model for the Mauritian PKI is illustrated below:



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.

The RA would be responsible for interfacing between the certificate holder and the CA and would be based in Mauritius. No certificates would be issued by the CA unless authorised by the RA. The entire PKI operation would be required to abide by international technical standards for facilitating interoperation of Mauritius PKI with PKIs of other countries. 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.

4. The operation of RCA and CA shall be governed by the legal and regulatory framework of Mauritius.

5. The infrastructure for RCA and CA shall meet the requirements as indicated in Schedule I on Information Technology (IT) Security Guidelines and in Schedule II on Security Guidelines for Certification Authorities.

6. The infrastructure of the RCA vendor should preferably meet standards/conditions prescribed by the browsers suppliers for getting the RCA public key included as a trusted key in browsers.

7. Tenderers shall comply with Schedule III on Standards followed by the Certification Authority. In addition the technologies, infrastructure both Hardware and Software, practices and procedures deployed by the Tenderer for the RCA and CA should conform to the relevant International Standards prescribed by IETF/NIST/FIPS/ITU/ISO/ANSI/IEC/PKCS. Compliance with the latest versions of the relevant standards will be preferred.

8. Tenderers shall have in place detailed manuals and shall ensure the scrupulous adherence to these manuals for performing all tasks.

9. Tenderers shall have a secure website complying with Schedule I, II and III. This website should be up and running on 24x7 basis. Planned exceptions should be notified on the website beforehand.

10. Tenderers for CA shall provide time stamping facility. Error of the time stamping clock shall not be more than 1 in 10^9.

11. Tenderers should be able to support dual key pairs PKI with independent expiry dates of two key pairs.

12. An Exclusive key pair of 2048 bits (for each key) shall be generated for the exclusive use by RCA. The private key of RCA shall be generated and kept in the Hardware Security Module (HSM) of security level FIPS 140-1 level 4. Representative(s) of the ICT Authority may be present during this key generation process. A self signed certificate shall be issued by RCA and displayed on the web site. The successful Tenderer shall provide an applet on his web site for facilitating the distribution of this self signed certificate to all certificate users and relying parties for verifying the trust chain up to RCA (Root) level. This applet shall be supplied to the ICT Authority and other authorised organisations to facilitate download from their web sites also. The applet shall be designed in a user-friendly manner.

13. An Exclusive key pair of 2048 bits (for each key) shall be generated for the exclusive use by CA. The private key of CA shall be generated and kept in the Hardware Security Module (HSM) of security level FIPS 140-1 level 4. Representative(s) of the ICT Authority may be present during this key generation Process. The public key of this key pair shall be submitted in PKCS 10 format to RCA for getting the PKC signed by RCA.

14. Use of RCA private key shall be completely off line. Computer systems containing HSM with RCA private key shall not be accessible at all from outside the operation room where these computer systems are housed. Proper electromagnetic and electrostatic shielding shall be provided in the operation room of RCA for the safety of RCA private key. It shall not be possible for anyone outside the operation room to read by any means /devices, the display/memory contents of any computer system within the operation room.

15. Video surveillance of all openings and other important areas shall be done on 24 x 7 basis. These shall be archived for a period of one year and shall be reviewed periodically by the authorised supervisor and the auditor.

16. Full back-up of the RCA private key in HSMs shall be available both at primary site and at off site with all security arrangements. Disaster recovery operation shall also be in place as per same Security Provisions available at the primary site.

17. Full back-up of the CA private key in HSMs shall be available both at primary site and at off site with all security arrangements. Disaster recovery operation shall be in place as per Security Standards.

18. Public key certificates of CAs shall be signed by the RCA, upon express authorisation of the ICT Authority only. This authorisation will be given to the vendor in electronic form with the digital signatures of authorised representatives of the ICT Authority and/or in the form of a paper document signed by the Controller or his authorised representative. This authorisation in electronic form and/or in paper form will have details including the public key of the CA. The successful Tenderer shall ensure that no public key certificate is issued to anybody without authorisation from the ICT Authority. The Controller may depute his representatives during the signing of the CA certificate.

19. CA shall provide two Registration Authorities (RAs) based in Mauritius .Each of these RA shall meet all requirements as described in Schedule IV “Requirements for Registration Authority (RA)”. The size of each key of the applicants’ key pair shall be 1024 bits. This key pair shall be generated on a hardware token like smart card or I-Key and the public key will be submitted to one of the RAs who shall request CA on internet/VPN in safe and secure way for getting the certificate issued to the applicant. The certificate shall be signed by the CA and issued to the applicant through the RA using internet/VPN. All communications between CA and RAs shall be encrypted to protect private data of the applicant. Necessary hardware and software for two RAs in Mauritius shall be included in the offer for CA by Tenderers. Details of hardware and software along with prices should be given clearly for two RAs in Mauritius.

20. CA shall issue certificates only upon express request(s) from the RA(s) in Mauritius.

21. Certificate life cycle management for the user certificates shall be done by the licensed CA through RAs in Mauritius.

22. CA shall always assure the confidentiality of applicants’ private information.

23. RCA will be required to cross certify other Roots or other CAs under specific authorisation of the ICT Authority. RCA shall have features so that all CAs whose PKCs have been signed by RCA should be able to inter-operate seamlessly.

24. RCA shall do the signing operations only on working days excluding Saturdays, Sundays and public holidays. At least three persons shall be needed for signing operation by RCA private key. The operation room can be securely locked but when open, at least two persons shall be present there.

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.

26. Certificates and CRLs shall be maintained on a separate server as an Authentication Database for CAs whose Public Key Certificates have been signed by RCA. This server shall be configured in fault tolerant mode to ensure uninterrupted availability of Repositories and CRLs.

27. CA shall ensure the continued accessibility and availability of all public key certificates and CRLs in its repository to its subscribers and relying parties.

28. CA shall update its certificates list and CRLs as soon as possible preferably deploying “Online Certificates Status Protocol" (OCSP).

29. CA shall ensure that the subscriber or any relying party can verify the CA Public Key Certificate by having access to the self signed PKC of RCA.

30. All certificates issued to CAs, repository of all certificates and CRLs shall be displayed, as per standards, on the website.

31. All submissions of PKCs and CRLs by CA to the repository of RCA must ensure that subscribers and relying parties are able to access the repository of RCA using LDAP ver.3 for X500 directories.

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.

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.

34. The Licensed CA 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 of this section on I.T Security guidelines for vendor’s facilities housing CA and the website. All these logs shall be analysed by the vendor for vulnerability assessment every year. Any shortcomings found shall be attended to and the Licensed CA shall be kept informed.

35. 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.

36. The vendor operating RCA shall not use the signing private key for any purpose without the specific authorisation of the ICT Authority. The vendor shall be fully responsible and accountable for signing certificates or revoking certificates or for any other uses of RCA private key which were not authorised by the ICT Authority.

37. Sensitive documents and materials shall be shredded before disposal. Media used to collect or transmit sensitive information shall be rendered unreadable before disposal. HSM and related devices shall be physically destroyed in accordance with the manufacturers’ guidance prior to disposal.

38. Tenderers shall make **all** software modules current by regular upgrading with the latest updates released by suppliers.

39. Notwithstanding any of the above provisions, the ICT Authority may issue such instructions as may be deemed appropriate for the operation of PKI services. These instructions shall be complied with.

SCHEDULE I

Information Technology (IT) Security Guidelines

Index

10. Audit Trails and Verification

11. Measures to Handle Computer Virus

12. Relocation of Hardware and Software

13. Hardware and Software Maintenance

14. Purchase and Licensing of Hardware and Software

15. System Software

16. Documentation Security

17. Network Communication Security

18. Firewalls

19. Connectivity

20. Network Administrator

21. Change Management

21.1 Change Control

21.2 Testing of Changes to Production System

21.3 Review of Changes

22. Problem Management and Reporting

23. Emergency Preparedness

24. Contingency Recovery Equipment and Services

25. Security Incident Reporting and Response

26. Disaster Recovery/Management

1 Introduction

This document provides guidelines for the implementation and management of Information Technology Security. Due to the inherent dynamism of the security requirements, this document does not provide an exact template for the vendors to follow. However, appropriate suitable samples of security process are provided for guidelines. It is the responsibility of the vendors to have in place internal processes that meet the guidelines set forth in this document.

The following words used in the Information Technology Security Guidelines shall be interpreted as follows:

- **shall**: The guideline defined is a mandatory requirement, and therefore must be complied with.
- **should**: The guideline defined is a recommended requirement. Non-compliance shall be documented and approved by the management. Where appropriate, compensating controls shall be implemented.
- **must**: The guideline defined is a mandatory requirement, and therefore must be complied with.
- **may**: The guideline defined is an optional requirement. The implementation of this guideline is determined by the organisation's requirement.

2. Implementation of an Information Security Programme

Successful implementation of a meaningful Information Security Programme rests with the support of the top management. Until and unless the senior managers of the organisation understand and concur with the objectives of the information security programme its ultimate success is in question.

The Information Security Programme should be broken down into specific stages as follows:

a) Adoption of a security policy

b) Security risk analysis

c) Development and implementation of an information classification system

d) Development and implementation of the security standards manual

e) Implementation of the management security self-assessment process

f) On-going security programme maintenance and enforcement

g) Training

h) Periodic Security audits by a reputed Information Technology security auditor

The principal task of the security implementation is to define the responsibilities of persons within the organisation. The implementation should be based on the general principle that the person who is generating the information is also responsible for its security. However, in order to enable him to carry out his responsibilities in this regard, proper tools, and the proper environment need to be established.

When different pieces of information at one level are integrated to form higher value information, the responsibility for its security needs also should go up in the hierarchy to the integrator and should require higher level of authority for its access. It should be absolutely clear for every information as to who are its owner, its custodian, and its users. It is the duty of the owner to assign the right classification to the information so that the required level of security can be enforced. The custodian of information is responsible for the proper implementation of security guidelines and making the information available to the users on a need to know basis.

3. Information Classification

Information assets must be classified according to their sensitivity and their importance to the organisation. Since it is unrealistic to expect managers and employees to maintain absolute control over all information within the boundaries of the organisation, it is necessary to advise them on which types of information are considered more sensitive, and how the organisation would like the sensitive information handled and protected. Classification, declassification, labelling, storage, access, destruction and reproduction of classified data and the administrative overhead this process will create must be considered. Failure to maintain a balance between the value of the information classified and the administrative burden the classification system places on the organisation will result in long-term difficulties in achieving success.

a) **Confidential** is that classification of information, the unauthorised disclosure of which could cause serious damage to the organisation, e.g. Strategic planning documents.

b) **Restricted** is that classification of information, the unauthorised disclosure of which would not be in the best interest of the organisation and/or its customers, e.g. Design details, computer software (programs, utilities), documentation, organisation personnel data, and budget information.

c) **Internal use** is that classification of information that does not require any degree of protection against disclosure within the company, e.g. Operating procedures, policies and standards inter office memorandums.

d) **Unclassified** is that classification of information that requires no protection against disclosure; for example**,** published annual reports, periodicals. While the above classifications are appropriate from a general organisation view point, the following classifications may be considered:

e) **Top secret -** it shall be applied to information, the unauthorised disclosure of which could be expected to cause exceptionally grave damage to the national security or national interest. This category is reserved for the nation's closest secrets and is to be used with great reserve.

f) **Secret -** this shall be applied to information, the unauthorised disclosure of which could be expected to cause serious damage to the national security or national interest or cause serious embarrassment in its functioning. This classification should be used for highly important information and is the highest classification normally used.

g) **Confidentiality -** this shall be applied to information unauthorised disclosure of which could be expected to cause damage to the security of the organisation or could be prejudicial to the interest of the organisation, or could affect the organisation in its functioning. Most information will on proper analysis be classified no higher than confidential.

h) **Restricted -** this shall be applied to information which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose.

i) **Unclassified -** this is the classification of information that requires no protection against disclosure.

4. Physical and Operational Security

4.1. Site Design

a) The site shall not be in locations that are prone to natural or man-made disasters, like flood, fire, chemical contamination and explosions.

b) As per the nature of the operations, suitable floor structuring, lighting, power and water damage protection requirements shall be provided.

c) Construction shall comply with all applicable building and safety regulations as laid down by the relevant Government agencies. Further, the construction must be tamper-evident.

d) Materials used for the construction of the operational site shall be fire-resistant and free of toxic chemicals.

e) External walls shall be constructed of reinforced concrete of sufficient thickness to resist forcible attack. Ground level windows shall be fortified with sturdy mild steel grills or impact-resistant laminated security glass. All internal walls must be from the floor to the ceiling and must be tamper-evident.

f) Air-conditioning system, power supply system and uninterrupted power supply unit with proper backup shall be installed depending upon the nature of operation. All ducting holes of the air-conditioning system must be designed so as to prevent intrusion of any kind.

g) Automatic fire detection, fire suppression systems and equipment in compliance with requirements specified by the authorised/competent agencies shall be installed at the operational site.

h) Media library and electrical and mechanical control rooms shall be housed in separate isolated areas, with access granted only to specific, named individuals on a need basis.

i) Any facility that supports mission-critical and sensitive applications must be located and designed for reparability, relocation and reconfiguration. The ability to relocate, reconstitute and reconfigure these applications must be tested as part of the business continuity/disaster recovery plan.

4.2. Fire Protection

a) Combustible materials shall not be stored within hundred metres of the operational site.

b) Automatic fire detection, fire suppression systems and audible alarms as prescribed by the authorised/competent agency shall be installed at the operational site.

c) Fire extinguishers shall be installed at the operational site and their locations clearly marked with appropriate signs.

d) Periodic testing, inspection and maintenance of the fire equipment and fire suppression systems shall be carried out.

e) Procedures for the safe evacuation of personnel in an emergency shall be visibly displayed at prominent places at the operational site. Periodic training and fire drills shall be conducted.

f) There shall be no eating, drinking or smoking in the operational site. The work areas shall be kept clean at all times.

4.3. Environmental Protection

a) Water detectors shall be installed under the raised floors throughout the operational site and shall be connected to audible alarms.

b) The temperature and humidity condition in the operational site shall be monitored and controlled periodically.

c) Personnel at the operational site shall be trained to monitor and control the various equipment and devices installed at the operational site for the purpose of fire and environment protection.

d) Periodic inspection, testing and maintenance of the equipment and systems shall be scheduled.

4.4. Physical Access

a) Responsibilities round the clock, seven days a week, three hundred sixty five days a year for physical security of the systems used for operation and also actual physical layout at the site of operation shall be defined and assigned to named individuals.

b) Biometric physical access security systems shall be installed to control and audit access to the operational site.

c) Physical access to the operational site at all times shall be controlled and restricted to authorised personnel only. Personnel authorised for limited physical access shall not be allowed to gain unauthorised access to restricted area within operational site.

d) Dual control over the inventory and issue of access cards/keys during normal business hours to the Data Centre shall be in place. An up-to-date list of personnel who possess the cards/keys shall be regularly maintained and archived for a period of three years.

e) Loss of access cards/keys must be immediately reported to the security supervisor of the operational site who shall take appropriate action to prevent unauthorised access.

f) All individuals, other than operations staff, shall sign in and sign out of the operational site and shall be accompanied by operations staff.

g) Emergency exits shall be tested periodically to ensure that the access security systems are operational.

h) All opening of the Data Centre should be monitored round the clock by surveillance video cameras.

5. Information Management

5.1. System Administration

a) Each organisation shall designate a properly trained "System Administrator" who will ensure that the protective security measures of the system are functional and who will maintain its security posture. Depending upon the complexity and security needs of a system or application, the System Administrator may have a designated System Security Administrator who will assume security responsibilities and provide physical, logical and procedural safeguards for information.

b) Organisations shall ensure that only a properly trained System Security Administrator is assigned the system security responsibilities.

c) The responsibility to create, classify, retrieve, modify, delete or archive information must rest only with the System Administrator.

d) Any password used for the system administration and operation of trusted services must not be written down (in paper or electronic form) or shared with any one. A system for password management should be put in place to cover the eventualities such as forgotten password or changeover to another person in case of System Administrator (or System Security Administrator) leaving the organisation. Every instance of usage of the administrator's passwords must be documented.

e) Periodic review of the access rights of all users must be performed.

f) The System Administrator must promptly disable access to a user's account if the user is identified as having left the Data Centre, changed assignments, no longer requires system access. Reactivation of the user's account must be authorised in writing by the System Administrator (Digitally signed e-mail may be acceptable).

g) The System Administrator must take steps to safeguard classified information as prescribed by its owner.

h) The System Administrator must authorise privileged access to users only on a need-to-know and need-to-do basis and also only after the authorisation is documented.

i) Criteria for the review of audit trails/access logs, reporting of access violations and procedures to ensure timely management action/response shall be established and documented.

j) All security violations must be recorded, investigated, and periodic status reports compiled for review by the management.

k) The System Administrator together with the system support staff shall conduct a regular analysis of problems reported and identify any weaknesses in the protection of the information.

l) The System Administrator shall ensure that the data, file and Public Key Infrastructure (PKI) servers are not left unmonitored while these systems are powered on.

m) The System Administrator should ensure that no generic user is enabled or active on the system.

n) The system administrator shall ensure the availability of the back up system when required.

5.2. Sensitive Information Control

a) Information assets shall be classified and protected according to their sensitivity and criticality to the organisation.

b) Procedures in accordance with subsection.8.3 of these Guidelines must be in place to handle the storage media, which has sensitive and classified information.

c) All sensitive information stored in any media shall bear or be assigned an appropriate security classification.

d) All sensitive material shall be stamped or labelled accordingly.

e) Storage media (i.e. floppy diskettes, magnetic tapes, portable hard disks, optical disks, etc.) containing sensitive information shall be secured according to their classification.

f) Electronic communication systems, such as router, switches, network device and computers, used for transmission of sensitive information should be equipped or installed with suitable security software and if necessary with an encryptor or encryption software. The appropriate procedure in this regard should be documented.

g) Procedures shall be in place to ensure the secure disposal of sensitive information assets on all corrupt/damaged or affected media both internal (e.g. hard disk/optical disk) and external (e.g. diskette, disk drive, tapes etc.) to the system. Preferably such affected/corrupt/damaged media both internal and external to the system shall be destroyed.

5.3. Sensitive Information Security

a) Highly sensitive information assets shall be stored on secure removable media and should be in an encrypted format to avoid compromise by unauthorised persons.

b) Highly sensitive information shall be classified in accordance with subsection 3 of this schedule.

c) Sensitive information and data, which are stored on the fixed disk of a computer shared by more than one person, must be protected by access control software (e.g., password). Security packages must be installed which partition or provide authorisation to segregated directories/files.

d) Removable electronic storage media must be removed from the computer and properly secured at the end of the work session or workday.

e) Removable electronic storage media containing sensitive information and data must be clearly labelled and secured.

f) Hard disks containing sensitive information and data must be securely erased prior to giving the computer system to another internal or external department or for maintenance.

5.4. Third Party Access

a) Access to the computer systems by other organisations shall be subjected to a similar level of security protection and controls as in these Information Technology security guidelines.

b) In case the Data Centre uses the facilities of an external service/facility provider (outsourcer) for any of their operations, the use of the external service/facility providers (e.g. outsourcer) shall be evaluated in the light of the possible security exposures and risks involved and all such agreements shall be approved by the information asset owner. The external service or facility provider shall also sign non-disclosure agreements with the management of the Data Centre/ operational site.

c) The external service/facility provider (e.g. outsourcer) shall provide an equivalent level of security controls as required by these Information Technology Security

Guidelines.

5.5. Prevention of Computer Misuse

a) Prevention, detection, and deterrence measures shall be implemented to safeguard the security of computers and computer information from misuse. The measures taken shall be properly documented and reviewed regularly.

b) Each organisation shall provide adequate information to all persons, including management, system developers and programmers, end-users, and third party users warning them against misuse of computers.

c) Effective measures to deal expeditiously with breaches of security shall be established within each organisation. Such measures shall include:

(i) Prompt reporting of suspected breach

(ii) Proper investigation and assessment of the nature of suspected breach

(iii) Secure evidence and preserve integrity of such material as relates to the discovery of any breach

(iv) Remedial measures

d) All incidents related to breaches shall be reported to the System Administrator or System Security Administrator for appropriate action to prevent future occurrence.

e) Procedure shall be set-up to establish the nature of any alleged abuse and determine the subsequent action required to be taken to prevent its future occurrence. Such procedures shall include:

(i) The role of the System Administrator, System Security Administrator and management

(ii) Procedure for investigation

(iii) Areas for security review

(iv) Subsequent follow-up action

6. System integrity and security measures

6.1. Use of Security Systems or Facilities

a) Security controls shall be installed and maintained on each computer system or computer node to prevent unauthorised users from gaining entry to the information system and to prevent unauthorised access to data.

b) Any system software or resource of the computer system should only be accessible after being authenticated by access control system.

6.2. System Access Control

a) Access control software and system software security features shall be implemented to protect resources. Management approval is required to authorise issuance of user identification (ID) and resource privileges.

b) Access to information system resources like memory, storage devices etc., sensitive utilities and data resources and programme files shall be controlled and restricted based on a "need-to-use" basis with proper segregation of duties.

c) The access control software or operating system of the computer system shall provide features to restrict access to the system and data resources. The use of common passwords such as "administrator" or "president" or "game" etc. to protect access to the system and data resources represents a security exposure and shall be avoided. All passwords used must be resistant to dictionary attacks.

d) Appropriate approval for the request to access system resources shall be obtained from the System Administrator. Guidelines and procedures governing access authorisations shall be developed, documented and implemented.

e) An Access Control System manual documenting the access granted to different levels of users shall be prepared to provide guidance to the System Administrator for grant of access.

f) Each user shall be assigned a unique user ID. Adequate user education shall be provided to help users in password choice and password protection. Sharing of user IDs shall not be allowed.

g) Stored passwords shall be encrypted using internationally proven encryption techniques to prevent unauthorised disclosure and modification.

h) Stored passwords shall be protected by access controls from unauthorised disclosure and modification.

i) Automatic time-out for terminal inactivity should be implemented.

j) Audit trail of security-sensitive access and actions taken shall be logged.

k) All forms of audit trail shall be appropriately protected against unauthorised modification or deletion.

l) Where a second level access-control is implemented through the application system, password controls similar to those implemented for the computer system shall be in place.

m) Activities of all remote users shall be logged and monitored closely.

n) The facility to login as another user from one user's login shall be denied. However, the system should prohibit direct login as a trusted user (e.g. root in UNIX, administrator in Windows NT or Windows 2000). This means that there must be a user account configured for the trusted administrator. The system requires each trusted user to change his effective username to gain access to root and also to re-authenticate him before requesting access to privileged functions.

o) The start-up and shutdown procedure of the security software must be automated.

p) Sensitive Operating System files, which are more prone to hackers, must be protected against all known attacks using proven tools and techniques. That is to say no user will be able to modify them except with the permission of System Administrator.

6.3. Password Management

a) Certain minimum quality standards for password shall be enforced. The quality level shall be increased progressively. The following control features shall be implemented for passwords:

(i) Minimum of eight characters without leading or trailing blanks;

(ii) Shall be different from the existing password and the two previous ones;

(iii) Shall be changed at least once every ninety days; for sensitive system, password shall be changed at least once every thirty days; and

(iv) Shall not be shared, displayed or printed.

b) Password retries shall be limited to a maximum of three attempted logons after which the user ID shall then be revoked; for sensitive systems, the number of password retries should be limited to a maximum of two.

c) Passwords which are easy-to-guess (e.g. user name, birth date, month, standard words etc.) should be avoided.

d) Initial or reset passwords must be changed by the user upon first use.

e) Passwords shall always be encrypted in storage to prevent unauthorised disclosure.

f) All passwords used must be resistant to dictionary attacks and all known password cracking algorithms.

6.4. Privileged User's Management

a) System privileges shall be granted to users only on a need-to-use basis.

b) Login privileges for highly privileged accounts should be available only from

Console and terminals situated within Console room.

c) An audit trail of activities conducted by highly privileged users shall be maintained for two years and reviewed periodically at least every week by an operator who is independent of the System Administrator.

d) Privileged user shall not be allowed to log in to the computer system from remote terminal. The usage of the computer system by the privilege user shall be allowed during a certain time period.

e) Separate user IDs shall be allowed to the user for performing privileged and normal (non-privileged) activities.

f) The use of user IDs for emergency use shall be recorded and approved. The passwords shall be reset after use.

6.5. User's Account Management

a) Procedures for user account management shall be established to control access to application systems and data. The procedures shall include the following:

(i) Users shall be authorised by the computer system owner to access the computer services.

(ii) A written statement of access rights shall be given to all users.

(iii) All users shall be required to sign an undertaking to acknowledge that they understand the conditions of access.

(iv) Where access to computer services is administered by service providers, ensure that the service providers do not provide access until the authorisation procedures have been completed. This includes the acknowledgment of receipt of the accounts by the users.

(v) A formal record of all registered users of the computer services shall be maintained.

(vi) Access rights of users who have been transferred, or left the organisation shall be removed immediately.

(vii) A periodic check shall be carried out for redundant user accounts and access rights that are no longer required.

(viii) Ensure that redundant user accounts are not re-issued to another user.

b) User accounts shall be suspended under the following conditions:

(i) When an individual is on extended leave or for inactive use of over thirty days. In the case of a protected computer system, the limit of thirty days may be reduced to fifteen days by the System Administrator.

(ii) Immediately upon the termination of the services of an individual.

(iii) Suspended or inactive accounts shall be deleted after a two months period. In case of protected computer systems, the limit of two months may be reduced to one month.

6.6. Data and Resource Protection

a) All information assets shall be assigned an "owner" responsible for the integrity of that data/resource. Custodians shall be assigned and shall be jointly responsible for information assets by providing computer controls to assist owners.

b) The operating system or security system of the computer system shall:

(i) Define user authority and enforce access control to data within the computer system;

(ii) Be capable of specifying, for each named individual, a list of named data objects (e.g. file, programme) or groups of named objects, and the type of access allowed.

c) For networked or shared computer systems, system users shall be limited to a profile of data objects required to perform their needed tasks.

d) Access controls for any data and/or resources shall be determined as part of the systems analysis and design process.

e) Application Programmer shall not be allowed to access the production system.

7. Sensitive Systems Protection

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.

b) For computer system processing sensitive data, access by other organisations shall be prohibited or strictly controlled.

c) For sensitive data, encryption of data in storage shall be considered to protect its confidentiality and integrity.

8. Data Centre Operations Security

8.1. Job Scheduling

a) Procedures shall be established to ensure that all changes to the job schedules are appropriately approved. The authority to approve changes to job schedules shall be clearly assigned.

b) As far as possible, automated job scheduling should be used. Manual job scheduling should require prior approval from the competent authority.

8.2. System Operations Procedure

a) Procedures shall be established to ensure that only authorised and correct job stream and parameter changes are made.

b) Procedures shall be established to maintain logs of system activities. Such logs shall be reviewed by a competent independent party for indications of dubious activities. Appropriate retention periods shall be set for such logs.

c) Procedures shall be established to ensure that people other than well-trained computer operators are prohibited from operating the computer equipment.

d) Procedures shall be implemented to ensure the secure storage or distribution of all outputs/reports, in accordance with procedures defined by the owners for each system.

8.3. Media Management

a) Responsibilities for media library management and protection shall be clearly defined and assigned.

b) All media containing sensitive data shall be stored in a locked room or cabinets, which must be fire resistant and free of toxic chemicals.

c) Access to the media library (both on-site and off-site) shall be restricted to the authorised persons only. A list of personnel authorised to enter the library shall be maintained.

d) The media containing sensitive and back up data must be stored at three different physical locations in the country, which can be reached within a few hours.

e) A media management system shall be in place to account for all media stored on-site and off-site.

f) All incoming/outgoing media transfers shall be authorised by management and users.

g) An independent physical inventory check of all media shall be conducted at least every six months.

h) All media shall have external volume identification. Internal labels shall be fixed, where available.

i) Procedures shall be in place to ensure that only authorised addition/removal of media from the library is allowed.

j) Media retention periods shall be established and approved by management in accordance with legal/regulatory and user requirements.

8.4. Media Movement

a) Proper records of all movements of computer tapes/disks between on-site and off-site media library must be maintained.

b) There shall be procedures to ensure the authorised and secure transfer to media to/from external parties and the off-site location. A means to authenticate the receipt shall be in place.

c) Computer media that are being transported to off-site data backup locations should be stored in locked carrying cases that provide magnetic field protection and protection from impact while loading and unloading and during transportation.

9. Data Backup and Off-site Retention

a) Back-up procedures shall be documented, scheduled and monitored.

b) Up-to-date backups of all critical items shall be maintained to ensure the continued provision of the minimum essential level of service. These items include:

(i) Data files
(ii) Utilities programmes
(iii) Databases
(iv) Operating system software
(v) Applications system software
(vi) Encryption keys
(vii) Pre-printed forms
(viii) Documentation (including a copy of the business continuity plans)

c) One set of the original disks for all operating system and application software must be maintained to ensure that a valid, virus-free backup exists and is available for use at any time.

d) Backups of the system, application and data shall be performed on a regular basis. Backups should also be made for application under development and data conversion efforts.

e) Data backup is required for all systems including personal computers, servers and distributed systems and databases.

f) Critical system data and file server software must have full backups taken weekly.

g) The backups must be kept in an area physically separate from the server. If critical system data on the LAN represents unique versions of the information assets, then the information backups must be rotated on a periodic basis to an off-site storage location.

h) Critical system data and file server software must have incremental backups taken daily.

i) Systems that are completely static may not require periodic backup, but shall be backed up after changes or updates in the information.

j) Each LAN/system should have a primary and backup operator to ensure continuity of business operations.

k) The business recovery plan should be prepared and tested on an annual basis.

10. Audit Trails and Verification

a) Transactions that meet exception criteria shall be completely and accurately highlighted and reviewed by personnel independent of those that initiate the transaction.

b) Adequate audit trails shall be captured and certain information needed to determine sensitive events and pattern analysis that would indicate possible fraudulent use of the system (e.g. repeated unsuccessful logons, access attempts over a series of days) shall be analysed. This information includes such information as who, what, when, where, and any special information such as:

(i) Success or failure of the event

(ii) Use of authentication keys, where applicable

c) Automated or manual procedures shall be used to monitor and promptly report all significant security events, such as accesses, which are out-of- pattern relative to time, volume, frequency, type of information asset, and redundancy. Other areas of analysis include:

(i) Significant computer system events (e.g. configuration updates, system crashes)

(ii) Security profile changes

(iii) Actions taken by computer operations, system administrators, system programmers, and/or security administrators

d) The real time clock of the computer system shall be set accurately to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.

e) The real time clock of the computer or communications device shall be set to the local time. Further there shall be a procedure that checks and corrects drift in the real time clock.

f) Computer system access records shall be kept for a minimum of two years, in either hard copy or electronic form. Records, which are of legal nature and necessary for any legal requirement or investigation of criminal behaviour, shall be retained as per the laws of the land.

g) Computer records of applications transactions and significant events must be retained for a minimum period of two years or longer depending on specific record retention requirements.

11. Measures to Handle Computer Virus

a) Responsibilities and duties shall be assigned to ensure that all file servers and personal computers are equipped with up-to-date virus protection and detection software.

b) Virus detection software must be used to check storage drives both internal and external to the system on a periodic basis.

c) All diskettes and software shall be screened and verified by virus detection software before being loaded onto the computer system. No magnetic media like tape cartridge, floppies etc. brought from outside shall be used on the data, file, PKI or computer server or personal computer on Intranet and Internet without proper screening and verification by virus detection software.

d) Representative(s) shall be designated to deal with reported or suspected incidents of computer virus. The designated representative(s) shall ensure that latest version of anti- virus software is loaded on all data, file, PKI servers and personal computers.

e) Procedures shall be established to limit the spread of viruses to other organisation information assets. Such procedures inter alia shall include:

(i) Communication to other business partners and users who may be at risk from an infected resource

(ii) Eradication and recovery procedures

(iii) Incident report must be documented and communicated as per established procedures.

f) An awareness and training programme shall be established to communicate virus protection practices, available controls, areas of high risk to virus infection and responsibilities.

12. Relocation of Hardware and Software

Whenever computers or computer peripherals are relocated (e.g. for maintenance, installation at different sites or storage), the following guidelines shall apply:

a) All removable media will be removed from the computer system and kept at a secure location.

b) Internal drives will be overwritten, reformatted or removed as the situation may be.

c) If applicable, ribbons will be removed from printers.

d) All paper will be removed from printers.

13. Hardware and Software Maintenance

Whenever, the hardware and software maintenance of the computer or computer network is being carried out, the following should be considered:

a) Proper placement and installation of Information Technology equipment to reduce the effects of interference due to electromagnetic emanations.

b) Maintenance of an inventory and configuration chart of hardware.

c) Identification and use of security features implemented within hardware.

d) Authorisation, documentation, and control of change made to the hardware.

e) Identification of support facilities including power and air conditioning.

f) Provision of an uninterruptible power supply.

g) Maintenance of equipment and services.

h) Organisation must make proper arrangements for maintenance of computer hardware, software (both system and application) and firmware installed and used by them. It shall be the responsibility of the officer in charge of the operational site to ensure that a contract for annual maintenance of hardware is always in place.

i) Organisation must enter into maintenance agreements, if necessary, with the supplier of computer and communication hardware, software (both system and application) and firmware.

j) Maintenance personnel will sign non-disclosure agreements.

k) The identities of all hardware and software vendor maintenance staff should be verified before allowing them to carry out maintenance work.

l) All maintenance personnel should be escorted within the operational site/ computer system and network installation room by the authorised personnel of the organisation.

m) After maintenance, any exposed security parameters such as passwords, user IDs, and accounts will be changed or reset to eliminate any potential security exposures.

n) If the computer system, computer network or any of its devices is vulnerable to computer viruses as a result of performing maintenance, system managers or users shall scan the computer system and its devices and any media affected for viruses as a result of maintenance.

14. Purchase and Licensing of Hardware and Software

a) Hardware and software products that contain or are to be used to enforce security, and intended for use or interface into any organisation system or network, must be verified to comply with these Information Technology Security Guidelines prior to the signing of any contract, purchase or lease.

b) Software, which is capable of bypassing or modifying the security system or operating system, integrity features, must be verified to determine that they conform to these Information Technology Security Guidelines. Where such compliance is not possible, then procedures shall be in place to ensure that the implementation and operation of that software does not compromise the security of the system.

c) There shall be procedures to identify, select, implement and control software (system and application software) acquisition and installation to ensure compliance with the Mauritian Copyright Act and Information Technology Security Guidelines.

d) It is prohibited to knowingly install on any system whether test or production, any software which is not licensed for use on the specific systems or networks.

e) No software will be installed and used on the system when appropriate licensing agreements do not exist, except during evaluation periods for which the user has documented permission to install and test the software under evaluation.

f) Illegally acquired or unauthorised software must not be used on any computer, computer network or data communication equipment. In the event that any illegally acquired or unauthorised software is detected by the System Administrator or Network Administrator, the same must be removed immediately.

15. System Software

a) All system software options and parameters shall be reviewed and approved by the management.

b) System software shall be comprehensively tested and its security functionality validated prior to implementation.

c) All vendor supplied default user IDs shall be deleted or password changed before allowing users to access the computer system.

d) Versions of system software installed on the computer system and communication devices shall be regularly updated.

e) All changes proposed in the system software must be appropriately justified and approved by an authorised party.

f) A log of all changes to system software shall be maintained, completely documented and tested to ensure the desired results.

g) Procedures to control changes initiated by vendors shall be in accordance with subsection 21 of this schedule pertaining to "Change Management".

h) There shall be no standing "Write" access to the system libraries. All "Write" access shall be logged and reviewed by the System Administrator for dubious activities.

i) System Programmers shall not be allowed to have access to the application system's data and programme files in the production environment.

j) Procedures to control the use of sensitive system utilities and system programmes that could bypass intended security controls shall be in place and documented. All usage shall be logged and reviewed by the System Administrator and another person independent of System Administrator for dubious activities.

16. Documentation Security

a) All documentation pertaining to application software and sensitive system software and changes made therein shall be updated to the current time, accurately and stored securely. An up-to-date inventory list of all documentation shall be maintained to ensure control and accountability.

b) All documentation and subsequent changes shall be reviewed and approved by an independent authorised party prior to issue.

c) Access to application software documentation and sensitive system software documentation shall be restricted to authorised personnel on a "need-to-use" basis only.

d) Adequate backups of all documentation shall be maintained and a copy of all critical documentation and manuals shall be stored off-site.

e) Documentation shall be classified according to the sensitivity of its contents/ implications.

f) Organisations shall adopt a clean desk policy for papers, diskettes and other documentation in order to reduce the risks of unauthorised access, loss of and damage to information outside normal working hours.

17. Network Communication Security

a) All sensitive information on the network shall be protected by using appropriate techniques. The critical network devices such as routers, switches and modems should be protected from physical damage.

b) The network configuration and inventories shall be documented and maintained.

c) Prior authorisation of the Network Administrator shall be obtained for making any changes to network configuration. The changes made in the network configuration shall be documented. The threat and risk assessment of the network after changes in the network configuration shall be reviewed. The network operation shall be monitored for any security irregularity. A formal procedure should be in place for identifying and resolving security problems.

d) Physical access to communications and network sites shall be controlled and restricted to authorised individuals only in accordance with subsection 4.4 of this schedule pertaining to "Physical Access".

e) Communication and network systems shall be controlled and restricted to authorised individuals only in accordance with subsection.6.2 of this schedule – System Access Control.

f) As far as possible, transmission medium within the Certification Authority's operational site should be secured against electro magnetic transmission. In this regard, use of Optical Fibre Cable and armoured cable may be preferred as transmission media as the case may be.

g) Network diagnostic tools, e.g., spectrum analyser, protocol analyser should be used on a need basis.

18. Firewalls

a) Intelligent devices generally known as "Firewalls" shall be used to isolate organisation's data network with the external network. Firewall device should also be used to limit network access for unauthorised use.

b) Networks that operate at varying security levels shall be isolated from each other by appropriate firewalls. The internal network of the organisation shall be physically and logically isolated from Internet and any other external connection by a firewall.

c) All firewalls shall be subjected to thorough test for vulnerability prior to being put to use and at least half-yearly thereafter.

d) All web servers for access by Internet users shall be isolated from other data and host servers.

19. Connectivity

a) Organisation shall establish procedure for allowing connectivity of their computer network or computer system to non-organisation computer system or networks. The permission to connect other networks and computer system shall be approved by the Network Administrator and documented.

b) All unused connections and network segments should be disconnected from active networks. The computer system/personal computer or outside terminal accessing an organisation's host system must adhere to the general system security and access control guidelines.

c) The suitability of new hardware/software particularly the protocol compatibility should be assessed before connecting the same to the organisation's network.

d) As far as possible, no Internet access should be allowed to database server/ file server or server hosting sensitive data.

e) The level of protection for communication and network resources should be commensurate with the criticality and sensitivity of the data transmitted.

20. Network Administrator

a) Each organisation shall designate a properly trained "Network Administrator" who will be responsible for operation, monitoring security and functioning of the network.

b) Network Administrator shall regularly undertake the review of network and also take adequate measures to provide physical, logical and procedural safeguards for its security. Appropriate follow up of any unusual activity or pattern of access on the computer network shall be investigated promptly by the Network Administrator.

c) System must include a mechanism for alerting the Network Administrator of possible breaches in security, e.g., unauthorised access, virus infection and hacking.

d) Secure Network Management System should be implemented to monitor functioning of the computer network. Broadcast of network traffic should be minimised.

e) Only authorised and legal software shall be used on the network.

f) Shared computer systems, network devices used for business applications shall comply with the requirement established in subsection 6 of this schedule – System Integrity and Security Measures.

21. Change Management

21.1. Change Control

a) Procedures for tracking and managing changes in application software, system software, hardware and data in the production system shall be established. Organisational responsibilities for the change management process shall be defined and assigned.

b) A risk and impact analysis, classification and prioritisation process shall be established.

c) No changes to a production system shall be implemented until such changes have been formally authorised. Authorisation procedures for change control shall be defined and documented.

d) Owners/Users shall be notified of all changes made to production system which may affect the processing of information on the said production system.

e) Fall-back procedures in the event of a failure in the implementation of the change process shall be established and documented.

f) Procedures to protect, control access and changes to production source code, data, execution statements and relevant system documentation shall be documented and implemented.

g) Version changes of application software and all system software installed on the computer systems and all communication devices shall be documented. Different versions of application software and system software must be kept in safe custody.

21.2. Testing Of Changes To Production System

a) All changes in computer resource proposed in production system shall be tested and test results shall be reviewed and accepted by all parties prior to implementation.

b) All user acceptance tests in respect of changes in computer resource in production system shall be performed in a controlled environment which includes:

(i) Test objectives

(ii) A documented test plan

(iii) acceptance criteria

21.3. Review Of Changes

a) Procedures shall be established for an independent review of programme changes before they are moved into a production environment to detect unauthorised or malicious codes.

b) Procedures shall be established to schedule and review the implementation of the changes in computer resource in the production system so as to ensure proper functioning.

c) All emergency changes/fixes in computer resource in the production system shall be reviewed and approved.

d) Periodic management reports on the status of the changes implemented in the computer resourced in the production system shall be submitted for management review.

22. Problem Management and Reporting

a) Procedures for identifying, reporting and resolving problems, such as non-functioning of Certification Authority's system; breaches in Information Technology security; and hacking, shall be established and communicated to all personnel concerned. It shall include emergency procedures. Periodic reports shall be submitted for management review.

b) A help desk shall be set up to assist users in the resolution of problems.

c) A system for recording, tracking and reporting the status of reported problems shall be established to ensure that they are promptly managed and resolved with minimal impact on the user of the computing resources.

23. Emergency Preparedness

a) Emergency response procedures for all activities connected with computer operation shall be developed and documented. These procedures should be reviewed periodically.

b) Emergency drills should be held periodically to ensure that the documented emergency procedures are effective.

24. Contingency Recovery Equipment and Services

a) Commitment shall be obtained in writing from computer equipment and supplies vendors to replace critical equipment and supplies within a specified period of time following a destruction of the computing facility.

b) The business continuity plan shall be developed which inter alias include the procedures for emergency ordering of the equipment and availability of the services.

c) The need for backup hardware and other peripherals should be evaluated in accordance with business needs.

25. Security Incident Reporting and Response

a) All security related incidents must be reported to the central coordinator, appointed by the management to coordinate and handle security related incidents. This central coordinator shall be the single point of contact at the organisation.

b) All incidents reported, actions taken, follow-up actions, and other related information shall be documented.

c) Procedures shall be defined for dealing with all security related incidents, including malicious software, break-ins from networks, software bugs which compromised the security of the system.

26. Disaster Recovery/Management

a) Disaster recovery plan shall be developed, properly documented, tested and maintained to ensure that in the event of a failure of the information system or destruction of the facility, essential level of service will be provided. The disaster recovery framework should include:

(i) emergency procedures, describing the immediate action to be taken in case of a major incident

(ii) fall back procedure, describing the actions to be taken to relocate essential activities or support services to a backup site

(iii) restoration procedures, describing the action to be taken to return to normal operation at the original site

b) The documentation should include:

  (i) definition of a disaster;

  (ii) condition for activating the plan;

  (iii) stages of a crisis;

  (iv) who will make decisions in the crisis;

  (v) role of individuals for each component of the plan;

  (vi) composition of the recovery team; and

  (vii) decision making process for return to normal operation.

c) Specific disaster management plan for critical applications shall be developed, documented, tested and maintained on a regular basis.

d) Responsibilities and reporting structure shall be clearly defined which will take effect immediately on the declaration of a disaster.

e) Each component/aspect of the plan should have a person and a backup assigned to its execution.

f) Periodic training of personnel and users associated with computer system and network should be conducted defining their roles and responsibilities in the event of a disaster.

g) Test plan shall be developed, documented and maintained. Periodic tests shall be carried out to test the effectiveness of the procedures in the plan. The results of the tests shall be documented for management review.

h) Disaster recovery plan should be updated regularly to ensure its continuing effectiveness.

SCHEDULE-II

Security Guidelines for Certification Authorities (CAs)

Index

18.4. Usage

18.5. Certification Authority's Public Key Delivery to Users

19. Private Key Protection and Backup

20. Method of Destroying Private Key

21. Usage Periods for the Public and Private Keys

21.1 Key Change

21.2 Destruction

21.3 Key Compromise

21.4 Cross-Certification

21.5 Revocation of Cross-Certified CA

22. Confidentiality of Subscriber's Information

23. Periodic Audit

1. Introduction

This document prescribes security guidelines for the management and operation of Certification Authorities (CAs) and is aimed at protecting the integrity, confidentiality and availability of their services, data and systems. These guidelines apply to Certification Authorities that perform all the functions associated with generation, issue and management of Digital Signature Certificate such as:

a) Verification of registration, suspension and revocation request;

b) Generation, issuance, suspension and revocation of Digital Signature Certificates; and

c) Publication and archival of Digital Signature Certificates, suspension and revocation of information.

2. Security Management

The Certification Authority shall define Information Technology security policies for its operation on the lines defined in Schedule-I. The policy shall be communicated to all personnel and widely published throughout the organisation to ensure that the personnel follow the policies.

3. Physical controls – site location, construction and physical access

a) The site location, design, construction and physical security of the operational site of Certification Authority shall be in accordance with subsection 4 of the Information Technology Security Guidelines given at Schedule-I in this section.

b) Physical access to the operational site housing computer servers, PKI server, communications and network devices shall be controlled and restricted to the authorised individuals only in accordance with subsection 4.4 of the Information Technology Security Guidelines given at Schedule-I in this section.

c) A Certification Authority must:

(i) ensure that the operational site housing PKI servers, communications and networks is protected with fire suppression system in accordance with subsection 4.2 of the Information Technology Security Guidelines given at Schedule-I of this section.

(ii) ensure that power and air-conditioning facilities are installed in accordance with subsection 4.1 of the Information Technology Security Guidelines given at Schedule-I of this section.

(iii) ensure that all removable media and papers containing sensitive or plain text information are listed, documented and stored in a container properly identified.

(iv) ensure unescorted access to Certification Authority's server is limited to those personnel identified on an access list.

(v) ensure that the exact location of Digital Signature Certification System shall not be publicly identified.

(vi) ensure that access security system is installed to control and audit access to the Digital Signature Certification System.

(vii) ensure that dual control over the inventory and access cards/keys are in place.

(viii) ensure that up-to-date list of personnel who possess the access cards/ keys is maintained at the Certification Authority's operational site. Loss of access cards/keys shall be reported immediately to the Security Administrator; who shall take appropriate actions to prevent unauthorised access.

(ix) ensure personnel not on the access list are properly escorted and supervised.

(x) ensure a site access log is maintained at the Certification Authority's operational site and inspected periodically.

d) Multi-tiered access mechanism must be installed at the Certification Authority's operational site. The facility should have clearly laid out security zones within its facility with well-defined access rights to each security zone. Each security zone must be separated from the other by floor to ceiling concrete reinforced walls. Alarm and intrusion detection system must be installed at every stage with adequate power backup capable of continuing operation even in the event of loss of main power. Electrical/Electronic circuits to external security alarm monitoring service (if used) must be supervised. No single person must have complete access to PKI Server, CA keys or any computer system or network device on his/her own.

e) Entrance to the main building where the Certification Authority's facilities such as Data Centre, PKI Server and Network devices are housed and entrance to each security zone must be video recorded round the clock. The recording should be carefully scrutinised and maintained for at least one year.

f) A Certification Authority site must be manually or electronically monitored for unauthorised intrusion at all times in accordance with the Information Technology Security Guidelines given at Schedule-I.

g) Computer System/PKI Server performing Digital Signature Certification function shall be located in a dedicated room or partition to facilitate enforcement of physical access control. The entry and exit of the said room or partition shall be automatically locked with time stamps and shall be reviewed daily by the Security Administrator.

h) Access to infrastructure components essential to operation of Certification Authority such as power control panels, communication infrastructure, Digital Signature Certification system, cabling, etc. shall be restricted to authorised personnel.

i) By-pass or deactivation of normal physical security arrangements shall be authorised and documented by security personnel.

j) Intrusion detection systems shall be used to monitor and record physical access to the Digital Signature Certification system during and after office hours.

k) Computer System or PKI Server performing the Digital Signature Certification functions shall be dedicated to those functions and should not be used for any other purposes.

l) System software shall be verified for integrity in accordance with subsection 15 of the Information Technology Security Guidelines given at Schedule-I of this section.

4. Media Storage

A Certification Authority must ensure that storage media used by his system are protected from environment threats such as temperature, humidity and magnetic and are transported and managed in accordance with subsection 8.3 and subsection 8.4 of the Information Technology Security Guidelines given at Schedule-I of this section.

5. Waste Disposal

All media used for storage of information pertaining to all functions associated with generation, production, issue and management of Digital Signature Certificate shall be scrutinised before being destroyed or released for disposal.

6. Off-site Backup

A Certification Authority must ensure that facility used for off-site backup, if any, shall be within the country and shall have the same level of security as the primary Certification Authority site.

7. Change and Configuration Management

a) The components of the Certification Authority infrastructure (e.g. cryptographic algorithm and its key parameters, operating system, system software, computer system, PKI server, firewalls, physical security, system security etc.) shall be reviewed every year for new technology risks and appropriate action plan shall be developed to manage the risks identified for each component.

b) The application software, system software and hardware, which are procured from questionable sources, shall not be installed and used for any function associated with generation and management of Digital Signature Certificate.

c) Software updates and patches shall be reviewed for security implications before being implemented on Certification Authority's system.

d) Software updates and patches to rectify security vulnerability in critical systems used for Certification Authority's operation shall be promptly reviewed and implemented.

e) Information on the software updates and patches and their implementation on Certification Authority's system shall be clearly and properly documented.

8. Network and Communications Security

a) Certification Authority's systems shall be protected to ensure network access control to critical systems and services from other systems in accordance with subsection 17, subsection 18, subsection 19 and subsection 20 of the Information Technology Security Guidelines given at Schedule-I of this section.

b) Network connections from the Certification Authority's system to external networks shall be restricted to only those connections which are essential to facilitate Certification Authority's functional processes and services. Such network connections to the external network shall be properly secured and monitored regularly.

c) Network connections should be initiated by the systems performing the functions of generation and management of Digital Signature Certificate to connect those systems performing the registration and repository functions but not vice versa. If this is not possible, compensating controls (e.g. use of proxy servers) shall be implemented to protect the systems performing the function of generation and management of Digital Signature Certificate from potential attacks.

d) Systems performing the Digital Signature Certification function should be isolated to minimise their exposure to attempts to compromise the confidentiality, integrity and availability of the certification function.

e) Communication between the Certification Authority systems connected on a network shall be secure to ensure confidentiality and integrity of the information. For example, communications between the Certification Authority's systems connected on a network should be encrypted and digitally signed.

f) Intrusion detection tools should be deployed to monitor critical networks and perimeter networks and alert administrators of network intrusions and penetration attempts in a timely manner.

g) Certificates and CRLs shall be maintained on a separate server which shall be configured in fault tolerant mode to ensure uninterrupted availability of all directories including CRL.

9. System Security Audit Procedures

9.1 Types of event recorded

a) The Certification Authority shall maintain record of all events relating to the security of his system. The records should be maintained in audit log file and shall include such events as:

(i) System start-up and shutdown;

(ii) Certification Authority's application start-up and shutdown;

(iii) Attempts to create, remove, set passwords or change the system privileges of the PKI Master Officer, PKI Officer, or PKI Administrator;

(iv) Changes to keys of the Certification Authority or any of his other details;

(v) Changes to Digital Signature Certificate creation policies, e.g. validity period;

(vi) Login and logoff attempts;

(vii) Unauthorised attempts at network access to the Certification Authority's system;

(viii) Unauthorised attempts to access system files;

(ix) Generation of own keys;

(x) Creation and revocation of Digital Signature Certificates;

(xi) Attempts to initialise remove, enable, and disable subscribers, and update and recover their keys;

(xii) Failed read-and-write operations on the Digital Signature Certificate and Certificate Revocation List (CRL) directory.

b) Monitoring and Audit Logs

(i) A Certification Authority should consider the use of automated security management and monitoring tools providing an integrated view of the security situation at any point in time. Records of the following application transactions shall be maintained:

i. Registration

ii. Certification;

iii. Publication;

iv. Suspension; and

v. Revocation.

(ii) Records and log files shall be reviewed regularly for the following activities:

i. Misuse;

ii. Errors;

iii. Security violations;

iv. Execution of privileged functions;

v. Change in access control lists;

vi. Change in system configuration.

c) All logs, whether maintained through electronic or manual means, should contain the date and time of the event, and the identity of the subscriber/ subordinate/entity which caused the event.

d) A Certification Authority should also collect and consolidate, either electronically or manually, security information which may not be generated by his system, such as:

i. Physical access logs;

ii. System configuration changes and maintenance;

iii. Personnel changes;

iv. Discrepancy and compromise reports;

v. Records of the destruction of media containing key material, activation data, or personal subscriber information.

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.

f) A Certifying Authority shall provide “Time Stamping” facility; the error of Time Stamping Clock shall not be more than 1 in $10^{9.}$

g) A Certification Authority should be able to generate the following reports:

(i) **Administrative operations reporting**

The system should be able to generate reports that describe all administrative operations performed.

(ii) **Certificates expiring report**

The system should be able to generate reports that describe all certificates that are within a specified period from expiry.

(iii) **Support for customisation of reports**

The system should support the generation of customisable reports.

9.2 Frequency of Audit Log Monitoring

The Certification Authority must ensure that its audit logs are reviewed by its personnel at least once every two weeks and all significant events are detailed in an audit log summary. Such reviews should involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Action taken following these reviews must be documented.

9.3. Retention Period for Audit Log

The Certification Authority must retain its audit logs onsite for at least twelve months and subsequently retain them in the manner described in subsection 10 of the Information Technology Security Guidelines as given in Schedule-I of this section.

9.4. Protection of Audit Log

The electronic audit log system must include mechanisms to protect the log files from unauthorised viewing, modification, and deletion. Manual audit information must be protected from unauthorised viewing, modification and destruction.

9.5. Audit Log Backup Procedures

Audit logs and audit summaries must be backed up or copied if in manual form.

9.6. Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. The Certification Authority must ensure that a vulnerability assessment is performed, reviewed and revised, if necessary, following an examination of these monitored events.

10. Records Archival

a) Digital Signature Certificates stored and generated by the Certification Authority must be retained for at least seven years after the date of its expiration. This requirement does not include the backup of private signature keys.

b) Audit information as detailed in subsection 9 of this schedule, subscriber agreements, verification, identification and authentication information in respect of subscriber shall be retained for at least seven years.

c) A second copy of all information retained or backed up must be stored at three locations within the country including the Certification Authority site and must be protected either by physical security alone, or a combination of physical and cryptographic protection. These secondary sites must provide adequate protection from environmental threats such as temperature, humidity and magnetism. The secondary site should be reachable in few hours.

d) All information pertaining to Subscriber's application, verification, identification, authentication and Subscriber agreement shall be stored within the country. This information shall be taken out of the country only with the permission of the ICT Authority and where a properly constitutional warrant or such other legally enforceable document is produced.

e) The Certification Authority should verify the integrity of the backups at least once every six months.

f) Information stored off-site must be periodically verified for data integrity.

11. Compromise and Disaster Recovery

11.1 Computing Resources, Software and/or Data are Corrupted

The Certification Authority must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing and networking resources, nominated website, repository, software and/or data. Where a repository is not under the control of the Certification Authority, the Certification Authority must ensure that any agreement with the repository provides for business continuity procedures.

11.2 Secure facility after a natural or other type of disaster

The Certification Authority must establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. Where a repository is not under the control of the Certification Authority, the Certification Authority must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.

11.3 Incident Management Plan

a) An incident management plan shall be developed and approved by the management. The plan shall include the following areas:

(i) Certification Authority's certification key compromise;

(ii) Hacking of systems and network;

(iii) Breach of physical security;

(iv) Infrastructure availability;

(v) Fraudulent registration and generation of Digital Signature Certificates;

(vi) Digital Signature Certificate suspension and revocation information.

b) An incident response action plan shall be established to ensure the readiness of the Certification Authority to respond to incidents. The plan should include the following areas:

(i) Compromise control;

(ii) Notification to user community; (if applicable)

(iii) Revocation of affected Digital Signature Certificates; (if applicable)

(iv) Responsibilities of personnel handling incidents;

(v) Investigation of service disruption;

(vi) Service restoration procedure;

(vii) Monitoring and audit trail analysis; and

(viii) Media and public relations.

12. Number of Persons Required Per Task

The Certification Authority must ensure that no single individual may gain access to the Digital Signature Certificate server and the computer server maintaining all information associated with generation, issue and management of Digital Signature Certificate and private keys of the Certification Authority. Minimum two individuals, preferably using a split-knowledge technique, such as twin passwords, must perform any operation associated with generation, issue and management of Digital Signature Certificate and application of private key of the Certification Authority.

13. Identification and Authentication for Each Role

All Certification Authority personnel must have their identity and authorisation verified before they are:

a) included in the access list for the Certification Authority's site;

b) included in the access list for physical access to the Certification Authority's system;

c) given a certificate for the performance of their Certification Authority role;

d) given an account on the PKI system.

Each of these certificates and accounts (with the exception of Certification Authority's signing certificates) must:

(i) be directly attributable to an individual;

(ii) not be shared;

(iii) be restricted to actions authorised for that role; and

(iv) procedural controls. Certification Authority's operations must be secured using techniques of authentication and encryption, when accessed across-a shared network.

14. Personnel Security Controls

The Certification Authority must ensure that all personnel performing duties with respect to its operation must:

a) be appointed in writing;

b) be bound by contract or statute to the terms and conditions of the position they are to fill;

c) have received comprehensive training with respect to the duties they are to perform;

d) be bound by statute or contract not to disclose sensitive Certification Authority's security related information or subscriber information;

e) not be assigned duties that may cause a conflict of interest with their Certification Authority's duties; and

f) be aware and trained in the relevant aspects of the Information Technology Security Policy and Security Guidelines framed for carrying out Certification Authority's operation.

15. Training Requirements

A Certification Authority shall ensure that all personnel performing duties with respect to its operation, must receive comprehensive training in:

a) relevant aspects of the Information Technology Security Policy and Security Guidelines framed by the Certification Authority;

b) all PKI software versions in use on the Certification Authority's system;

c) all PKI duties they are expected to perform; and

d) disaster recovery and business continuity procedures.

16. Retraining Frequency and Requirements

The requirements of subsection 15 of this schedule must be kept current to accommodate changes in the Certifying Authority's system. Refresher training must be conducted as and when required, and the Certification Authority must review these requirements at least once a year.

17. Documentation Supplied to Personnel

A Certification Authority must make available to his personnel the Digital Signature Certificate policies it supports, its Certification Practice Statement, Information Technology Security Policy and any specific statutes, policies or contracts relevant to their position.

18. Key Management

18.1 Generation

a) Integrity of CA private key is vital. It shall therefore be strong and shall be generated using unpredictable random number generators preferably hardware based.

b) The subscriber's key pair shall be generated by the subscriber or on a key generation system in the presence of the subscriber.

c) The key generation process shall generate statistically random key values that are resistant to known attacks.

d) The CA shall use the initialisation data provided in the Initialisation stage and then generate the key pair and submit the public key to the Root Authority in Standard format.

e) The CA shall have a process in place which shall verify that the user possesses the private key corresponding to the public key submitted to CA for issuance of the certificate.

18.2 Distribution of Keys

Keys shall be transferred from the key generation system to the storage device (if the keys are not stored on the key generation system) using a secure mechanism that ensures confidentiality and integrity.

18.3 Storage

a) Certification Authority's keys shall be stored in tamper-resistant devices and can only be activated under split-control by parties who are not involved in the set-up and maintenance of the systems and operations of the Certification Authority. The key of the Certification Authority may be stored in a tamper- resistant cryptographic module or split into sub-keys stored in tamper-resistant devices under the custody of the key custodians.

b) The Certification Authority's key custodians shall ensure that the Certification Authority's key component or the activation code is always under his sole custody. Change of key custodians shall be approved by the Certification Authority's management and documented.

18.4 Usage

a) A system and software integrity check shall be performed prior to Certification Authority's key loading.

b) Custody of and access to the Certification Authority's keys shall be under split control. In particular, Certification Authority's key loading shall be performed under split control.

18.5 Certification Authority's Public Key Delivery to Users

The Certification Authority's public verification key must be delivered to the prospective Digital Signature Certificate holder in an on-line transaction, in accordance with PKIX-3 Certificate Management Protocol, or via an equally secure manner.

19. Private Key Protection and Backup

a) The Certification Authority must protect its private keys from disclosure. The CA shall ensure the continued availability of the private key in the event of loss or corruption of the private key.

b) The Certification Authority must back-up its private keys. Backed-up keys must be stored in encrypted form and protected at a level no lower than those followed for storing the primary version of the key.

c) The Certification Authority's private key backups should is stored in a secure storage facility, away from where the original key is stored.

20. Method of Destroying Private Key

Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space must be securely destroyed by over-writing. Private key destruction procedures must be described in the Certification Practice Statement or other publicly available document.

21. Usage Periods for the Public and Private Keys

21.1 Key Change

a) Certification Authority and Subscriber keys shall be changed periodically.

b) Key change shall be processed as per Key Generation guidelines.

c) The Certification Authority shall provide reasonable notice to the Subscriber's relying parties of any change to a new key pair used by the Certification Authority to sign Digital Signature Certificates.

d) The Certification Authority shall define its key change process that ensures reliability of the process by showing how the generation of key interlocks – such as signing a hash of the new key with the old key.

All keys must have validity periods of no more than ten years.

Suggested validity period:

a) Certification Authority's root keys and associated certificates – seven years;

b) Certification Authority's private signing key –seven years;

c) Subscriber Digital Signature Certificate key – three years;

d) Subscriber private key – three years.

Key lengths for keys in (a) above shall not be less than 2048 bits and for others it shall not be less than 1024 bits.

21.2 Destruction

Upon termination of use of a Certification Authority signature private key, all components of the private key and all its backup copies shall be securely destroyed.

21.3 Key Compromise

a) A procedure shall be pre-established to handle cases where a compromise of the Certification Authority's Digital Signature private key has occurred. In such case, the Certification Authority shall immediately revoke all affected Subscriber Digital Signature Certificates.

b) The Certification Authority should immediately revoke the affected keys and Digital Signature Certificates in the case of Subscriber private key compromise.

c) The Certification Authority's public keys shall be archived permanently to facilitate audit or investigation requirements.

d) Archives of Certification Authority's public keys shall be protected from unauthorised modification.

21.4 Cross Certification

The CA shall be able to support the following:

a) Peer to Peer cross certification

b) Multi level hierarchical cross-certification

c) Unidirectional cross certification

d) Bi-directional cross certification

e) Cross-certification through Root

21.5 Revocation of a CA

The CA shall be able to revoke a cross certified CA. In case of revocation of the Certificate of the CA itself, all certificates issued by that CA shall be put in the CRL immediately.

22. Confidentiality of Subscriber's Information

a) Procedures and security controls to protect the privacy and confidentiality of the subscribers' data under the Certification Authority's custody shall be implemented. Confidential information provided by the subscriber must not be disclosed to a third party without the subscribers' consent, unless the information is required to be disclosed under the law or a court order.

b) Data on the usage of the Digital Signature Certificates by the subscribers and other transactional data relating to the subscribers' activities generated by the Certification Authority in the course of its operation shall be protected to ensure the subscribers' privacy.

c) A secure communication channel between the Certification Authority and its subscribers shall be established to ensure the authenticity, integrity and confidentiality of the exchanges (e.g. transmission of Digital Signature Certificate, password, private key) during the Digital Signature Certificate issuance process.

23. Periodic Audit

The Certification Authority shall subject itself to periodic audits to ensure that provisions of Schedule-I, Schedule-II & Schedule-III are complied by it. As the cryptographic components of the Certification Authority systems are highly sensitive and critical, components must be subjected to periodic expert review to ensure their integrity and assurance.

SCHEDULE-III

The standards followed by the Certification Authority

(1) Every Certification Authority shall observe the following standards for carrying out different activities associated with its functions.

(a) **PKIX (Public Key Infrastructure)**

Public Key Infrastructure as recommended by Internet Engineering Task Force (IETF) document updated for “Internet X.509 Public Key Infrastructure”.

(b) **Public-key cryptography based on the emerging Institute of Electrical and Electronics Engineers (IEEE) standard P1363 for three families:**

Discrete Logarithm (DL) systems
Elliptic Curve Discrete Logarithm (EC) systems
Integer Factorisation (IF) systems;

(c) **Public-key Cryptography Standards (PKCS)**

PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit)
PKCS#3 Diffie-Hellman Key Agreement Standard
PKCS#5 Password Based Encryption Standard
PKCS#6 Extended-Certificate Syntax Standard
PKCS#7 Cryptographic Message Syntax standard
PKCS#8 Private Key Information Syntax standard
PKCS#9 Selected Attribute Types
PKCS#10 RSA Certification Request
PKCS#11 Cryptographic Token Interface Standard
PKCS#12 Portable format for storing/transporting a user’s private keys and certificates
PKCS#13 Elliptic Curve Cryptography Standard
PKCS#15 Cryptographic Token Information Format Standard;

(d) **Federal Information Processing Standards (FIPS)**

FIPS 180-1, Secure Hash Standard
FIPS 186-1, Digital Signature Standard (DSS)
FIPS 140-1 level 4, Security Requirement for Cryptographic Modules (HSMs);

(e) **Discrete Logarithm (DL) systems**

Diffie-Hellman, MQV key agreement
DSA, Nyberg-Rueppel signatures;

(f) **Elliptic Curve (EC) systems**

Elliptic curve analogs of DL systems;

(g) **Integer Factorisation (IF) systems**

RSA encryption
RSA, Rabin-Williams signatures;

(h) **Key agreement schemes**

(i) **Signature schemes**
DL/EC scheme with message recovery
PSS, FDH, PKCS #1 encoding methods for IF family
PSS-R for message recovery in IF family;
(ii) **Encryption schemes**
Abdalla-Bellare-Rogaway DHAES for DL/EC family;

(i) **Form and size of the key pairs**

(1) The minimum key length for Asymmetric cryptosystem (RSA Algorithm) shall be 2048 bits for the Certification Authority's key pairs and 1024 for the key pairs used by subscribers.
(2) The Certification Authority's key pairs shall be changed every three to five years (except during exigencies as in the case of key compromise when the key shall be changed immediately). The Certification Authority shall take appropriate steps to ensure that key changeover procedures as mentioned in Schedule I & Schedule II are adhered to.
(3) The subscriber's key pairs shall be changed every two to three years;

(j) **Directory Services**
Both X-500 and LDAP v3 shall be supported. X.500 for publication of Public Key Certificates and Certificate Revocation Lists X.509 version 3 Certificates as specified in ITU RFC 1422 X.509 version 2 Certificate Revocation Lists;

(i) **Publication of Public Key Certificate.**
The Certification Authority shall, on acceptance of a Public Key Certificate by a subscriber, publish it on its web site for access by the subscribers and relying parties. The Certification Authority shall be responsible and shall ensure the transmission of Public Key Certificates and Certificate Revocation Lists to the National Repository of RCA (Root Certification Authority), for access by subscribers and relying parties. The National Repository shall conform to X.500 Directory Services and provide for access through LDAP Ver. 3. The Certification Authority shall be responsible for ensuring that Public Key Certificates and Certificate Revocation Lists integrate seamlessly with the National Repository on their transmission;

(k)**Public Key Certificate Standard**

All Public Key Certificates issued by the Certification Authorities shall conform to International Telecommunication Union X.509 version 3 standard. X.509 v3 certificate basic syntax is as follows.

tbsCertificate

```
{
    Version
    Serial Number
    Signature
    Issuer
    Validity
    Subject
    Subject Public Key Information
    Issuer Unique ID [1] IMPLICIT Unique Identifier optional,
              — If present, version shall be v2 or v3
    Subject Unique ID [2] IMPLICIT Unique Identifier optional,
              — If present, version shall be v2 or v3
    Extensions        [3] EXPLICIT Extensions optional
            —  If present, version shall be v3
{

         Authority Key Identifier
        {
            Key Identifier optional,
            Authority Certificate Issuer optional,
            Authority Certificate Serial Number optional
        }
        Subject Key Identifier
        Key Usage
        {
            Digital Signature
            Non Repudiation
            Key Encipherment
            Data Encipherment
            Key Agreement
            Key Cert Sign
            cRLSign
            Encipher Only
            Decipher Only
        }
        Private Key Usage Period
        {
            Not Before optional,
            Not After optional
        }
        Certificate Policies
        {
            Policy Information
            {
                Policy Identifier
                Policy Qualifiers optional
            }
            Certificate Policy Id
            {
                Policy Qualifier Info
                {
```

```
            Policy Qualifier Id
            Qualifier
            {
                cPSuri
                User Notice
                {
                    Notice Reference optional
                    {
                        Organisation
                        Notice Numbers
                    }
                    Display Text optional
                    {
                        visibleString
                        bmpString
                        utf8String
                    }
Policy Mappings
{
    Issuer Domain Policy
    Subject Domain Policy
}
Subject Alternative Name
{
    General Name
    {
        Other Name
        {

         type-id
         value
        }
        Rfc822Name
        DNS Name
        X400 Address
        Directory Name
        edi Party Name
        {
        Name Assigner optional,
        Party Name
        }
        Uniform Resource Identifier
        IP Address
        Registered ID
    }
}
Issuer Alternative Names
Subject Directory Attributes
Basic Constraints
{
    cA
    path Len Constraint optional
}

Name Constraints
{
    Permitted Subtrees optional
    Excluded Subtrees optional
}
Policy Constraints
{
    Require Explicit Policy optional
    Inhibit Policy Mapping optional
}
Extended key usage field
{
    Extended Key Usage Syntax
    Key Purpose Id
    {
        Server Authentication
        Client Authentication
        Code Signing
        Email Protection
        Time Stamping
    }
}
CRL Distribution Points
{
    CRL Distribution Points Syntax
    Distribution Point
    {
        Distribution Point optional
        {
            full Name
            name Relative To CRL Issuer
        }
    }
    Reasons  optional
    {
        Unused
        Key Compromise
        CA Compromise
        Affiliation Changed
        Superseded
        Cessation Of Operation
        Certificate Hold
    }
    cRL Issuer optional
}
Authority Information Access
{
    Authority Information Access Syntax
```

```
         Access Description
         {
           Access Method
           Access Location
         }
       }
Signature Algorithm
Signature Value
}
```

(i) **Certificate**

TBSCertificate is certificate “to be signed”. The field contains the names of the subject and issuer, a public key associated with the subject, a validity period, and other associated information. The fields are described in detail.

(ii) **Version**

This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, use X.509 version 3(value is 2). If no extensions are present, but a Unique Identifier is present, use version 2 (value is 1). If only basic fields are present, use version 1 (the value is omitted from the certificate as the default value).

(iii) **Serial number**

The serial number is an integer assigned by the Certification Authority to each certificate. It shall be unique for each certificate issued by a given Certification Authority (i.e., the issuer name and serial number identify a unique certificate).

(iv) **Signature**

This field contains the algorithm identifier for the algorithm used by the Certification Authority to sign the certificate.

(v) **Issuer**

The issuer field identifies the entity who has signed and issued the certificate. The issuer field shall contain a non-empty distinguished name.

(vi) **Validity**

The certificate validity period is the time interval during which the Certification Authority warrants that it will maintain information about the status of the certificate.

(vii) **Subject**

The subject field identifies the entity associated with the public key stored in the subject public key field. The subject name may be carried in the subject field and/or the subjectAltName extension. If the subject is a Certification Authority (e.g., the basic constraints extension, is present and the value of cA is TRUE,) then the subject field shall be populated with a non-empty distinguished name matching the contents of the issuer field in all certificates issued by the subject Certification Authority.

(viii) Subject Public Key Information

This field is used to carry the public key and identify the algorithm with which the key is used.

(ix) Unique Identifiers

These fields may only appear if the version is 2 or 3. The subject and issuer unique identifiers are present in the certificate to handle the possibility of reuse of subject and/or issuer names over time.

(x) Extensions

This field may only appear if the version is 3. The extensions defined for X.509 v3 certificates provide methods for associating additional attributes with users or public keys and for managing the certification hierarchy. The X.509 v3 certificate format also allows communities to define private extensions to carry information unique to those communities. If present, this field is a sequence of one or more certificate extensions. The content of certificate extensions in the Internet Public Key Infrastructure is defined as follows, namely:-.

(a) Authority Key Identifier

The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate. This extension is used where an issuer has multiple signing keys (either due to multiple concurrent key pairs or due to changeover). The identification may be based on either the key identifier (the subject key identifier in the issuer's certificate) or on the issuer name and serial number.

(b) Subject Key Identifier

The subject key identifier extension provides a means of identifying certificates that contain a particular public key.

(c) Key Usage

The key usage extension defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate. The usage restriction might be employed when a key that could be used for more than one operation is to be restricted. For example, when an RSA key should be used only for signing, the digital Signature and/or non-Repudiation bits would be asserted. Likewise, when an RSA key *should be used only for key management, the key Encipherment bit would be asserted.*

(d) Private Key Usage Period

The private key usage period extension allows the certificate issuer to specify a different validity period for the private key than the certificate. This extension is intended for use with digital signature keys. This extension consists of two optional components, not Before and not After. (This profile recommends against the use of this extension. Certification Authorities conforming to this profile MUST NOT generate certificates with critical private key usage period extensions.)

(e) Certificate Policies

The certificate policies extension contains a sequence of one or more policy information terms, each of which consists of an object identifier and optional qualifiers. These policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used. Optional qualifiers, which may be present, are not expected to change the definition of the policy.

(f) Policy Mappings

This extension is used in Certification Authority certificates. It lists one or more pairs of object identifiers; each pair includes an issuer Domain Policy and a subject Domain Policy. The pairing indicates the issuing Certification Authority considers its issuer Domain Policy equivalent to the subject Certification Authority's subject Domain Policy.

(g) Subject Alternative Name

The subject alternative names extension allows additional identities to be bound to the subject of the certificate. Defined options include an Internet electronic mail address, a Directory Naming Service name, an IP address, and a uniform resource identifier (URI).

(h) Issuer Alternative Names

This extension is used to associate Internet style identities with the certificate issuer.

(i) Subject Directory Attributes

The subject directory attributes extension is not recommended as an essential part of this profile, but it may be used in local environments.

(j) Basic Constraints

The basic constraints extension identifies whether the subject of the certificate is a Certification Authority and how deep a certification path may exist through that Certification Authority.

(k) Name Constraints

The name constraints extension, which MUST be used only in a Certification Authority certificate, indicates a name space within which all subject names in subsequent certificates in a certification path shall be located. Restrictions may apply to the subject distinguished name or subject alternative names. Restrictions apply only when the specified name form is present. If no name of the type is in the certificate, the certificate is acceptable.

(l) Policy Constraints

The policy constraints extension can be used in certificates issued to Certification Authorities. The policy constraints extension constrains path validation in two ways. It can be used to prohibit policy mapping or require that each certificate in a path contain an acceptable policy identifier.

(m)Extended key usage field

This field indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension field.

(n) CRL Distribution Points

The CRL distribution points extension identifies how CRL information is obtained.

(o) Private Internet Extensions

This extension may be used to direct applications to identify an on-line validation service supporting the issuing Certification Authority.

(p) Authority Information Access

The authority information access extension indicates how to access Certification Authority information and services for the issuer of the certificate in which the extension appears. Information and services may include on-line validation services and Certification Authority policy data.

(xi) Signature Algorithm

The Signature Algorithm field contains the identifier for the cryptographic algorithm used by the Certification Authority to sign this certificate. The algorithm identifier is used to identify a cryptographic algorithm.

(xii) Signature Value

The Signature Value field contains a digital signature computed upon the Abstract Syntax Notation (ASN.1) DER encoded tbsCertificate. The ASN.1 DER encoded tbsCertificate is used as the input to the signature function. This signature value is then ASN.1 encoded as a BIT STRING and included in the Certificate's signature field.

(l) Certificate Revocation List Standard –

CRL and CRL Extensions Profile - The CRL contents as per International Telecommunications Union standard ver 2 are as follows

```
CertificateList
    {
      TBSCertList
        {
        Version
        Signature
        Issuer
        This Update
        Next Update
        Revoked Certificates
          {

          User Certificate
          Revocation Date
              Certificate Revocation List Entry Extensions
              {
              Reason Code
                {
                  Unspecified
                  Key Compromise
                  CA Compromise
                  Affiliation Changed
                  Superseded
                  Cessation Of Operation
                  Certificate Hold
                  Remove From Certificate Revocation List
                }
                Hold Instruction Code
                Invalidity Date
                Certificate Issuer
          }  optional
          Certificate Revocation List Extensions
          {
          Authority Key Identifier
          Issuer Alternative Name
          Certificate Revocation List Number
          Delta Certificate Revocation List Indicator
          Issuing Distribution Point
          {
```

```
                    Distribution Point
                    Only Contains User Certs
                    Only Contains CA Certs
                    Only Some Reasons
                    Indirect Certificate Revocation List
                 }
                 }  optional
```

Signature Algorithm
Signature Value
}

(i) tbsCertList

The certificate list to be signed, or TBSCertList, is a sequence of required and optional fields. The required fields identify the Certificate Revocation List issuer, the algorithm used to sign the Certificate Revocation List, the date and time the Certificate. Revocation List was issued, and the date and time by which the Certification Authority will issue the next Certificate Revocation List. Optional fields include lists of revoked certificates and Certificate Revocation List extensions. The Revoked Certificate List is optional to support the case where a Certification Authority has not revoked any unexpired certificates that it has issued. The profile requires conforming Certification Authorities to use the Certificate Revocation List extension cRLNumber in all Certificate Revocation Lists issued. The first field in the sequence is the tbsCertList. This field is itself a sequence containing the name of the issuer, issue date, issue date of the next list, the list of revoked certificates, and optional Certificate Revocation List extensions. Further, each entry on the revoked certificate list is defined by a sequence of user certificate serial number, revocation date, and optional Certificate Revocation List entry extensions. The fields are described in detail, as follows namely:-

(ii) Version

This optional field describes the version of the encoded Certificate Revocation List. When extensions are used, as required by this profile, this field MUST be present and MUST specify version 2 (the integer value is 1).

(iii) Signature

This field contains the algorithm identifier for the algorithm used to sign the Certificate Revocation List. This field shall contain the same algorithm identifier as the signature Algorithm field in the sequence Certificate List.

(iv) Issuer Name

The issuer name identifies the entity who has signed and issued the Certificate Revocation List. The issuer identity is carried in the issuer name field. Alternative name forms may also appear in the issuer Alternate Name extension. The issuer name field MUST contain an X.500 distinguished name (DN). The issuer name field is defined as the X.501 type Name, and MUST follow the encoding rules for the issuer name field in the certificate.

(v) This Update

This field indicates the issue date of this Certificate Revocation List. This Update may be encoded as UTC Time or Generalised Time. Certification Authorities conforming to this profile and that issue Certificate Revocation Lists MUST encode This Update as UTCTime for dates through the year 2049. Certification Authorities conforming to this profile that issue Certificate Revocation Lists MUST encode This Update as Generalised Time for dates in the year 2050 or later.

(vi) Next Update

This field indicates the date by which the next Certificate Revocation List will be issued. The next Certificate Revocation List could be issued before the indicated date, but it will not be issued any later than the indicated date. Certification Authorities should issue Certificate Revocation Lists with a Next Update time equal to or later than all previous Certificate Revocation Lists. Next Update may be encoded as UTCTime or Generalised Time.

(vii) Revoked Certificates

Revoked certificates are listed. The revoked certificates are named by their serial numbers. Certificates revoked by the Certification Authority are uniquely identified by the certificate serial number. The date on which the revocation occurred is specified. Additional information may be supplied in Certificate Revocation List entry extensions;

(viii) CRL Entry Extensions

The Certificate Revocation List entry extensions already defined by American National Standards Institute X9 and International Standards Organisation /IEC / International Telecommunication Union for X.509 v2 Certificate Revocation Lists provide methods for associating additional attributes with Certificate Revocation List entries [X.509] [X9.55]. The X.509 v2 Certificate Revocation List format also allows communities to define private Certificate Revocation List entry extensions to carry information unique to those communities. All Certificate Revocation List entry extensions used in this specification are non-critical.

(a) Reason Code

The reason Code is a non-critical Certificate Revocation List entry extension that identifies the reason for the certificate revocation. Certification Authorities are strongly encouraged to include meaningful reason codes in Certificate Revocation List entries; however, the reason code Certificate Revocation List entry extension should be absent instead of using the unspecified (0) Reason Code value.

(b) Hold Instruction Code

The hold instruction code is a non-critical Certificate Revocation List entry extension that provides a registered instruction identifier, which indicates the action to be taken after encountering a certificate that has been placed on hold.

(c) Invalidity Date

The invalidity date is a non-critical Certificate Revocation List entry extension that provides the date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid. This date may be earlier than the revocation date in the Certificate Revocation List entry, which is the date at which the Certification Authority processed the revocation.

(d) Certificate Issuer

This Certificate Revocation List entry extension identifies the certificate issuer associated with an entry in an indirect Certificate Revocation List, i.e. a Certificate Revocation List that has the indirect Certificate Revocation List indicator set in its issuing distribution point extension. If this extension is not present on the first entry in an indirect Certificate Revocation List, the certificate issuer defaults to the Certificate Revocation List issuer. On subsequent entries in an indirect Certificate Revocation List, if this extension is not present, the certificate issuer for the entry is the same as that for the preceding entry.

(ix) Issuing Distribution Point

The issuing distribution point is a critical Certificate Revocation List extension that identifies the Certificate Revocation List distribution point for a particular Certificate Revocation List, and it indicates whether the Certificate Revocation List covers revocation for end entity certificates only, Certification Authority certificates only, or a limited set of reason codes. Although the extension is critical, conforming implementations are not required to support this extension.

(x) Signature Algorithm

The signature Algorithm field contains the algorithm identifier for the algorithm used by the Certification Authority to sign the Certificate List. This field MUST contain the same algorithm identifier as the signature field in the sequence tbsCertList.

(xi) Signature Value

The signature Value field contains a digital signature computed upon the ASN.1 DER encoded to be signed CertList. The ASN.1 DER encoded tbsCertList is used as the input to the signature function. This signature value is then ASN.1 encoded as a BIT STRING and included in the Certificate Revocation List's signature Value field.

SCHEDULE IV

REQUIREMENTS FOR REGISTRATION AUTHORITY (RA):

1. Registration Authority in Mauritius shall be able to do the following:

a) Identification of the applicant requesting for a public key certificate (PKC).

b) Verifications of the information supplied by the applicant.

c) Verifying the eligibility of the applicant for the class of certificate requested.

d) Verifying that the applicant is in possession of the private key corresponding to the public key he has submitted for the certificate.

e) Assigning unique name for the identification of the applicant.

2. In case the applicant wishes to use his own computer system the RA shall provide a suitable token (crypto smart card or I-Key) and the suitable driver (software) so that the applicant can generate the key-pair on the token and is able to submit the public key in proper PKCS format to the RA.

3. HARDWARE and SOFTWARE at RA end for secured communications between the applicants' system and the RA system shall be provided.

4. In case the applicant wishes to use the facilities of RA, the RA shall have secured facilities to generate the key pair on the suitable token (crypto smart card or I-Key) and give the token to the applicant with PKC installed.

5. Proper archiving shall be kept for all details about requests, messages sent to CA, the certificates received from the CA and the certificates handed over to users.

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.

7. Secured communications facilities shall be provided for all communications between RA and CA right from the receipt of application to the delivery of certificate to the applicant phases.

8. Facilities shall be provided for printing on smart cards. Details of the applicant including his photograph, serial number of the card, logo of the RA / CA etc. may be printed on the smart card.

9. Requests for issue of PKCs from CA shall be digitally signed by the authorised person of RA.

10. The operation of systems in RA should be secured by the biometric enabled identification of the authorised RA personnel in addition to his password.

11. There shall be no trace of applicants' Private Key on the system of RA or on the system of CA even when the applicant had used the RA facilities for generating the key pair on the crypto smart card or on the I-key.

12. RA shall support smart cards with crypto engine from the major smart cards manufactures.

13. RA shall support I-keys from the major I-key manufacturers.

14. Cost of supplying 200 crypto smart cards along with 200 smart card readers USB pluggable and 500 crypto i-keys shall be included in the price quoted for setting up of two RAs in Mauritius. These shall be supplied to the ICT Authority before starting the acceptance testing of RAs.

15. The RA shall be able to issue about 500 certificates per day on an 8 working hours per day basis.

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.

17. RA shall have secured systems deploying required firewalls, intrusion detection systems and other security measures.

18. RA shall also generate requests for certificate renewals and revocations.

19. The successful Tenderer has to ensure seamless working of RAs with the CA during the entire period of hosting of CA facilities. If during the contract period the CA upgrades or modifies its facilities the necessary upgrading of RAs in Mauritius, required for this seamless working, shall be the responsibility of the successful Tenderer and shall be implemented by him at no cost to the ICT Authority.

20. Both batch mode requests and single request from RAs to CA for issuing of PKCs shall be implemented.

21. All communications between RAs and CA shall follow relevant international standard formats like PKCS formats.

Section

D

D. ADDITIONAL DETAILS REQUIRED BY THE ICT AUTHORITY

ICT AUTHORITY

DOCUMENTS REQUIRED BY ICT AUTHORITY

TENDER NO.: ICTA/PKI-1/2004-2005

Tenderers are required to submit the following details as separate attachments to the tender response.

1. ATTACHMENT 1 - TENDERER CAPABILITY

1.1 TENDERER QUALIFICATIONS

a) It is required that the Tenderer should have previous experience in providing PKI services. Please describe your strength and experience as an operator in providing PKI services.

b) It is desirable that the Tenderer should have previous experience with providing PKI services. Please provide the list of organisations to which you are providing PKI services.

c) Please provide the audited annual reports for last 3 years for your company.

d) Describe the financial and technical resources that could be devoted to this project.

1.2 ABILITY TO PROVIDE SERVICES

Tenderers shall describe any plans for the next 12 months that could materially affect the ability to provide the services proposed in this RFP. Any contracts (for similar services as requested in this RFP) that have been cancelled or lawsuits (involving your ability or performance under such a contract) filed in which the Tenderer has been involved during the last two years, shall be disclosed.

2. ATTACHMENT 2 - IMPLEMENTATION PLAN

Tenderers shall describe how the project will be implemented, using existing infrastructure and processes. Additional infrastructure and processes to be added to meet the requirements of RCA and CA including two RAs in Mauritius, must also be included, along with any assumptions, restrictions, or constraints that might affect the implementation.

3. ATTACHMENT 3 - MAINTENANCE, SERVICE AND SUPPORT

Reliability and performance of the service will be essential for the growth of e-governance and e-commerce in Mauritius.

a) Provision of all PKI services for Mauritius shall be the responsibility of the successful Tenderer. Tenderers shall supply detailed descriptions of services including time stamping service, hours of availability, types of access restrictions if any, contact person details etc, for smooth and efficient running of RCA and CA including RAs in Mauritius.

b) Tenderers shall describe key management plans for CA signing keys.

c) Tenderers shall confirm the availability of support for a period extending over the next 3 years from Vendors/suppliers of your PKI. Successful Tenderer shall make vendor agreements available to the ICT Authority/licensed CA.

d) Tenderers shall include detailed description of the method for distribution of Root Certificate and/or CA certificates.

4. ATTACHMENT 4 - SERVICE LEVEL AGREEMENT

a) It is required that the successful bidder signs a service level agreement as part of the contract for providing quality PKI services. A copy of the proposed service level agreement must be included in the proposal.

b) The percentage uptime guaranteed overall for every PKI services proposed must be disclosed.

c) The time frame proposed for response to problems and problem resolving processes shall be detailed.

5. ATTACHMENT 5 - HANDING OVER OF PRIVATE KEY(S) AT THE END OF CONTRACT

a) Tenderers shall describe a secured procedure of handing over the private key(s) of RCA and/or CA to the ICT Authority at the end of the contract.

b) Tenderers shall describe the process of ensuring that no trace of private key(s) of RCA and/or CA is left with the Tenderer after the handing over of the private key(s) to the ICT Authority at the end of the contract.

6. ATTACHMENT 6 - TRAINING

Tenderers shall describe the training requirements in terms of optimum man power, duration, cost and place of training for each of the following (as applicable):

a) Operation and maintenance of RAs in Mauritius.

b) Operation and maintenance of directory hosting at the ICT Authority.

c) Operation and maintenance of time-stamping at the ICT Authority.

7. ATTACHMENT 7 - DETAILS OF INFRASTRUCTURE

Tenderers shall describe the proposed hardware modules, software modules, HSMs, directory services, processes in place or to be set up for each of the physical locations including those in Mauritius. Copies of relevant certificates for standards adhered to shall be included.

8. ATTACHMENT 8 – INTERWORKING OF RAs & CA

Tenderers shall state the maximum and average response time for issuing a PKC after the request for issuing the PKC had been accepted at the RA in Mauritius. Details about the connectivity (band-width) and other requirements between RA & CA shall be given clearly.

9. ATTACHMENT 9 – OPERATION AND MAINTENANCE MANUALS

Tenderers shall provide detailed manuals for operation and maintenance of RAs, time stamping facilities and directory hosting at the ICT Authority.

10. ATTACHMENT 8 - PRICING FOR PKI SERVICES

Tenderers shall provide the **breakdown** of the costs associated with **all components** (capital and recurring).

11. ATTACHMENT 9 - ADDITIONAL INFORMATION

Provide any additional information or background, which may be helpful to the persons reviewing your response.

Section

E

E. FINANCIAL SUMMARY SHEETS

- *Financial Summary Sheet I – Bid for RCA, CA and RAs*
- *Financial Summary Sheet II – Bid for RCA*
- *Financial Summary Sheet III – Bid for CA and RAs*

ICT AUTHORITY

FINANCIAL SUMMARY SHEET I

For Combined RCA, CA and RAs Tender

TENDER NO: ICTA/PKI-1/2004-2005

- The financial proposal should reflect all the costs involved for the solution quoted in the technical proposal.

- PKI services shall be provided and all related works shall be completed as per the information provided in the proposal and as per the tender specifications.

- Prices quoted in the Financial Summary sheet will be binding and should be supported by detailed calculations.

1. RCA Services & CA Services & Hosting of Directories on its Website

a) Facilities Outside Mauritius

One time charges (if any) *in words*: US Dollars ……………………………………………
……………………………………………………………… US $……...…………………

Recurring charges/annum *in words*: US Dollars ……………………………………………
………………………………………………………….. US $............………………..

b) Setting up of two RAs in Mauritius

One time charges (if any) *in words*: US Dollars ……………………………………………
……………………………………………………………… US $……...…………………

Recurring charges/annum *in words*: US Dollars ……………………………………………
………………………………………………………….. US $............………………..

2. Setting up of secured facilities (hardware & software) for hosting of directories at ICT Authority

One time charges (if any) *in words*: US Dollars ……………………………………………
……………………………………………………………… US $……...…………………

Recurring charges/annum *in words*: US Dollars ……………………………………………
………………………………………………………….. US $............………………..

3. **Setting up of facilities (hardware & software) for time-stamping at the ICT Authority in Mauritius**

One time charges (if any) *in words*: US Dollars ……………………………………………. ……………………………………………………………. US $……..……………………

Recurring charges/annum *in words*: US Dollars ……………………………………………. …………………………………………………………... US $.............……………….

4. **Operation and Maintenance Training for personnel of the concerned organisations**

Total Charges (if any) *in words* for training required to operate and maintain:

a) RAs

US Dollars ……………………………………………………………………………… …………………………………………………. US $……..…………………………

b) Directories

US Dollars ……………………………………………………………………………… …………………………………………………. US $……..…………………………

c) Time-stamping

US Dollars ……………………………………………………………………………… …………………………………………………. US $……..…………………………

Total recurring charges/year for next three years *in words* – US Dollars …………………………………………………………………………………………… and Total one time fixed charges *in words* - US Dollars……………………………………………………………………………………….

Signature: ……………………………………………………………………

Full name of Signatory………………………………………………………….

Phone number: …………………………………………………………..

Fax Number: ……………………………………………………………….

Address: ………………………………………………………………………

……………………………………………………………………………………

Date: ……………………………

Company's official Seal:

ICT AUTHORITY

FINANCIAL SUMMARY SHEET II

For RCA Tender

TENDER NO.: ICTA/PKI-1/2004-2005

- The financial proposal should reflect all the costs involved for the solution quoted in the technical proposal.

- PKI services shall be provided and all related works shall be completed as per the information provided in the proposal and as per the tender specifications.

- Prices quoted in the Financial Summary sheet will be binding and should be supported by detailed calculations.

1. **RCA Services & Hosting of Directories on its Website**

One time charges (if any) *in words*: US Dollars ……………………………………….
…………………………………………………………. US $……...…………………
Recurring charges/annum *in words*: US Dollars ……………………………………….
…………………………………………………………... US $............………………..

2. **Setting up of secured facilities (hardware & software) for hosting of directories at the ICT Authority**

One time charges (if any) *in words*: US Dollars ……………………………………….
…………………………………………………………. US $……...…………………
Recurring charges/annum *in words*: US Dollars ……………………………………….
…………………………………………………………... US $............………………..

3. **Operation and Maintenance Training for personnel of the concerned organisations**

Total Charges (if any) *in words* for training required to operate and maintain **directories:**

US Dollars …………………………………………………………………………………….

……………………………………………………. US $……...…………………………

Signature: ………………………………………………………………

Full name of Signatory…………………………………………………….

Phone number: …………………………………………………………..

Fax Number: …………………………………………………………….

Address: ………………………………………………………………

…………………………………………………………………………

Date: ……………………………

Company's official Seal:

ICT AUTHORITY

FINANCIAL SUMMARY SHEET III

For CA and RAs Tender

TENDER NO.: ICTA/PKI-1/2004-2005

- The financial proposal should reflect all the costs involved for the solution quoted in the technical proposal.

- PKI services shall be provided and all related works shall be completed as per the information provided in the proposal and as per the tender specifications.

- Prices quoted in the Financial Summary sheet will be binding and should be supported by detailed calculations.

5. CA Services & Hosting of Directories on its Website

a) Facilities Outside Mauritius

One time charges (if any) *in words*: US Dollars ……………………………………………

…………………………………………………………………. US $……...…………………

Recurring charges/annum *in words*: US Dollars ……………………………………………

………………………………………………………………….. US $.............………………..

b) Setting up of RAs in Mauritius

One time charges (if any) *in words*: US Dollars ……………………………………………

…………………………………………………………………. US $……...…………………

Recurring charges/annum *in words*: US Dollars ……………………………………………

………………………………………………………………….. US $.............………………..

6. Setting up of facilities (hardware & software) for time-stamping at the ICT Authority in Mauritius

One time charges (if any) *in words*: US Dollars ……………………………………………

…………………………………………………………………. US $……...…………………

Recurring charges/annum *in words*: US Dollars ……………………………………………

………………………………………………………………….. US $.............………………..

7. **Operation and Maintenance Training for personnel of the concerned organisations**

Total Charges (if any) *in words* for training required to operate and maintain:

a) **RAs**

US Dollars …………………………………………………………………………………

………………………………………………. US $……..…………………………

b) **Time-stamping**

US Dollars …………………………………………………………………………………

………………………………………………. US $……..…………………………

Total recurring charges/year for next three years *in words* – US Dollars ……………………………………………………………………………………… and Total one time fixed charges *in words* - US Dollars……………………………………………………………………………….

Signature: ……………………………………………………………….

Full name of Signatory…………………………………………………….

Phone number: ………………………………………………………..

Fax Number: ……………………………………………………….

Address: ……………………………………………………………….

………………………………………………………………………….

Date: ……………………………

Company's official Seal:

Section

F

F. FORM OF TENDER BOND

ICT AUTHORITY

TENDER BOND

TENDER NO.: ICTA/PKI-1/2004-2005

KNOW ALL MEN by these present that we, ……………………………………..… ……………………………………………..……..whose registered office is at ……………………………….……………(*hereinafter called* "***The Surety***'*)* are held and firmly bound unto the ………………….. (*hereinafter called* '***The Employer***'*)* in the sum of Mauritian Rupees One Hundred and Fifty Thousands only (Rs 150,000/) for the payment of which sum we bind ourselves, our successors and assigns jointly and severally by the presents.

WHEREAS..… whose registered office is at………………………………………………………… ………………………………………………………………………………….…….

(*hereinafter called* '***The Tenderer***') has, by a Tender (*hereinafter called the* '***Said Tender***') made to the Employer offered to enter into a contract, viz:-

CONTRACT for providing all PKI Services……………………………………………

………….as therein mentioned and has undertaken to enter into a ***Performance Bond*** for the due performance of the Contract should the said Tender be accepted by the Employer.

NOW THE CONDITION of this Bond is such that if the Tenderer shall maintain the said Tender and shall enter into a Contract, including the submission of a Performance Bond for the due performance of the Contract within 15 days of the date of notification of acceptance of the said Tender by the Employer, then this obligation shall be null and void but otherwise shall be and remain in full force and effect for a period of at least one hundred and eighty (180) days from the date of closing of the tender.

Dated at ....……..........… this ………………..………. day of ……......................... 2004.

Signature : ....

Name : ……………………………………

Status : ………………………………….

Witness : ....

Section

G

G. FORM OF AGREEMENT

ICT AUTHORITY

FORM OF AGREEMENT

AGREEMENT BETWEEN the ICT Authority (hereinafter called the Employer) represented by the Executive Director on the one part and...…………….. (hereinafter called the Contractor) on the other part.

WHEREAS the Employer is desirous that certain works should be executed, viz.:............................……………………….………………..................... the whole of the works as morefully described in the Contract Documents.

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

In this agreement words and expressions shall have the same meaning as are respectively assigned to them in the Conditions of Contract hereinafter referred to:

The following documents shall be deemed to form and be read and constructed as part of this Agreement, viz:

a) Letter of Award/acceptance

b) Instructions to Tenderers.

c) Forms of Tender

d) Specifications including four Schedules

e) Financial Summary sheets

f) Form of Performance Bond.

In consideration of the payments to be made by the Employer to the Contractor as hereinafter mentioned the Contractor hereby covenants with the Employer to construct, complete, maintain the works and provide PKI services in conformity in all respects with the provision of the contract.

The Employer hereby covenants to pay the Contractor, in consideration of the construction, completion, maintenance of the works and providing PKI Services for the sum of US Dollars .... (US $……………………) at the times and in the manner described in the contract.

Drawn up in duplicate and good faith on .... IN WITNESS hereof the parties hereto have caused their respective common seals to be hereunto affixed (or have hereunto set their respective hands and seals) the day and year first above written.

The common seal of .... Limited was hereunto affixed in the presence of:..

Or,

Signed, Sealed and Delivered by the said:

……………………………………………………………………………………………

in the presence of:...

Name :……………………………………………………………………………..

Address :……………………………………………………………………………..

……………………………………………………………………………

Description :……..

Signed by the said (Employer):

……………………………………………………………..

Name :……………………………………………………………………………..

Address :……………………………………………………………………………..

……………………………………………………………………………

Description :……..

Section
H

H. FORM OF PERFORMANCE BOND

ICT AUTHORITY

PERFORMANCE BOND

BY THIS BOND we, whose principal place of business (registered office) ………………………………………………………………………………………… is at ……………………………………………………………… (hereinafter called **"the Contractor"**) and ………………………………………………………………………………………… whose principal place of business (registered office) is at ……………………………………………… (hereinafter called **"the Sureties"**) are held and firmly bound unto the ICT Authority (hereinafter called **"the Employer")** in the sum of (**10% of Value of Contract**) ……………………………………………………… payment of which sum the Contractor and the Sureties bind themselves and their assigns jointly and severally by these presents.

Sealed with our respective seals and dated this………………………… day of ……………….2004

WHEREAS the Contractor by an Agreement made between the Employer of the one part and the Contractor of the other part has entered into a Contract viz ……………………………………………………………………………………………… (hereinafter called **"the Contract"**) for the supply, implementation and maintenance of the works and providing PKI services as therein mentioned in conformity with the provisions of the Said Contract.

NOW THE CONDITION OF THE ABOVE WRITTEN Bond is such that if the Contractor shall duly perform and observe all the terms, provisions, conditions and stipulations of the Contract on the Contractor's part to be performed and observed according to the true purport, intent and meaning thereof or if on default by the Contractor the Sureties shall satisfy and discharge the damages sustained by the Employer thereby up to the amount of the above written Bond then this obligation shall be null and void but otherwise shall be and remain in full force and effect but no alteration in terms of the Contract or in the extent or nature of the thereunder or in respect of the obligations to correct defects thereunder and no allowance of time by the Employer or the Project Officer under the Contract nor any forebearance or forgiveness in or in respect of any matter of thing concerning the Contract on the part of the Employer or the said Project Officer shall in any way release the Sureties from liability under the above written Bond.

THE COMMON SEAL OF)
was hereunto affixed)
in the presence of)

THE COMMON SEAL OF)
was hereunto affixed)
in the presence of)