Registration Authority (RA) Appointment Guideline

REVISION CONTROL AND CHANGE HISTORY

Revision Number	Approval Date	Approved by	Amendment
Rev. 0	3 Mac 2014	Amir Suhaimi Hassan	New document release
Rev. 1	22 Aug 2014	Amir Suhaimi Hassan	1. Include ISMS requirement on the document labelling 2. Change of document ID 3. Change of Department name from Compliance Div. to Compliance Dept. 4. Include reference to Documents and Records Control Procedure
Rev. 2	23 Aug 2017	Amir Suhaimi Hassan	Logo, address and contact details update

TABLE OF CONTENTS

PURPOSE

The Objective of the guidelines is to provide detailed requirements; terms and conditions on the appointment of a Registration Authority ("RA") and to ensure only competent RA will be appointed. This document shall be the sole reference for any company who intend to become an RA for Pos Digicert Sdn. Bhd. ("POS DIGICERT").

SCOPE

This document covers the detailed description and/or process flow for the following:

a) RA Requirements and Evaluation Criteria
b) Performance Bond
c) Legal Matters
d) Annual Review
e) Record Keeping
f) Audit Guidelines
g) Termination of RA

RELATED POLICY

Reference. No.	Title of Policy	Location
Clause 4.1	Quality Management System ISO 9001:2015	SI
DQMS-QM-01	Quality Manual	SI
DQMS-CS-SP101	Legal and Compliance Manual	LCD

LEGISLATIVE CONTEXT

Reference No.	Title of Document	Location
Nil	Nil	Nil

DEFINITIONS AND ACRONYMS

Word/Term	Definition
DSA 1997	Digital Signature Act 1997 (Act 562) is an Act to make provision for, and to regulate the use of, digital signature and to provide for matters connected therewith.
DSA 1998	Digital Signature Regulations 1998

1) DEFINITION OF REGISTRATION AUTHORITY (RA)

1.1 An RA is a trusted entity appointed by POS DIGICERT to assist subscribers in applying for digital certificates, to approve digital certificate requests and/or to assist POS DIGICERT in the revocation of digital certificates.

1.2 An RA will be seen as one of the contributory factors in the success of the business of a Certification Authority. To achieve this, a Registration Authority Guidelines shall be established to ensure standards are not compromised.

1.3 Functions of an RA includes (but not limited to):

a) Agent to process the application and revocation of digital certificates.

b) Responsible to embed the digital certificate on the media for the movement of physical items between an RA and POS DIGICERT (e.g. smart cards, USB Tokens & Medias).

c) Strictly adhere to the Standard Operating Procedures of an RA in the process of application, revocation, renewal and other matters pertaining to digital certificates.

2) RA REQUIREMENTS AND EVALUATION CRITERIA

The degree of trust provided by the licensed certificates used may vary. Thus, the required RA assessment will have to be set as per the actual practice definition to foster uniformity. POS DIGICERT will assess the status of an RA applicant based on the following criteria:

2.1 Types of Companies

a) Private
b) Public listed
c) Government controlled
d) Banking and financial institution
e) A company with a nationwide network would be an added advantage.

2.2 Capital Requirement

The company shall have a minimum paid-up capital of RM2.0 Million unimpaired by losses. Annual audited financial accounts of the company shall be submitted to POS DIGICERT for evaluation purposes. Notwithstanding the above, POS DIGICERT shall always reserve its right to amend the evaluation criteria on a case to case basis.

2.3 Company Performance and Image

The company's track record in terms of its profitability, management capabilities and public image will be the criteria in recommending the RA appointment.

2.4 Documentation Required

a) Application letter/form duly completed
b) Memorandum & Articles of Association
c) Form 49 – Particulars of Directors (duly certified by ROC)
d) Form 24 – Return on allotment of shares (duly certified by ROC)
e) Credit Reference from banking & financial institutions
f) Latest Audited Accounts (3 years)
g) Certified copy of the resolutions passed by the Board of Directors accepting the appointment and operations as a RA (upon approval by POS DIGICERT)

2.5 Operational Capabilities

2.5.1 Personnel

There are three different operative personnel. The requirements for operative personnel are as follows (unless waived in writing by POS DIGICERT):

2.5.1.1 RA Manager

RA Manager shall be responsible to ensure the followings:

a) Supervise and manage RA counters. He/she shall co-ordinate the job shifts among the Registration Officer (RO) and Registration Personnel (RP) to ensure that all operations are carried out in a proper manner and in accordance with pre-determined schedule.
b) Endeavour to solve any problems or difficulties faced by the RO and RP in the course of executing their functions.
c) Participate in any management meeting or decision making on behalf of the RA's company.
d) Shall handle all financial and commercial matters between an RA and POS DIGICERT.
e) May be qualified to act in the capacity of the RO except for instances of RA initiated revocation exercise.
f) Appointment of an RA Manager shall strictly comply with the following criteria:

i. Must be appointed by the authorized Executive of the RA company via an official letter *(refer Appendix 1)*
ii. He/she has completed higher education in the information technology field
iii. He/she has significant knowledge in the operation of the CA and RA (advantage)
iv. The RA company has conducted a background check on him/her against any criminal or fraudulent history

v. He/she signs the declaration on fraud cases and compliance with laws upon appointment as RA Manager (no specific format)

vi. He/she signs the bi-annual renewal of the declaration on fraud cases and compliance with laws (no specific format)

2.5.1.2 Registration Personnel

Among tasks of an RP are as below:

a) RP is the first person to come into contact with the applicant. He/she shall verify if the applicant has ever been blacklisted by the CA and then ensure the completeness of the application.

b) Verifies the identity of the applicant by physically sighting the applicant and compare against the original photograph identification documents.

c) Confirms payment of subscription fees before escalating the relevant documents to RO.

d) Appointment of an RP shall strictly comply with the following criteria:

i. Must be appointed by the authorized Executive of the RA company via an official letter *(refer Appendix 1)*

ii. He/she has knowledge in the information technology field

iii. He/she has significant knowledge in the operations of the CA and RA (advantage)

iv. The RA company has conducted a background check on him/her against any criminal or fraudulent history

2.5.1.3 Registration Officer

Among tasks of an RO are as below:

a) Perform validation procedures to ensure relevant documents are available and identity of applicant matches the identification documents.

b) To process the application of digital certificates

c) Accountable for the RO smart card, which is used to sign digital certificate issuance requests.

d) In charge of ensuring the availability of forms; stationary and other required equipment.

e) Appointment of an RO shall strictly comply with the following criteria:

i. Must be appointed by the authorized Executive of the RA company via an official letter *(refer Appendix 1)*
ii. He/she has completed higher education in the information technology field
iii. He/she has significant knowledge in the operations of the CA and RA (advantage)
iv. The RA company has conducted a background check on him/her against any criminal or fraudulent history

2.5.2 Training

a) The RA Operative Personnel will be required to attend training programs conducted by POS DIGICERT which include Certificate Management System (CMS) clients and all operational related matters.

b) POS DIGICERT shall provide the RA with relevant manuals and trainings. The overall costs will be borne by the RA.

2.5.3 Financial

The RA shall be required to comply with the agreed payment terms, mechanism, related financial policies and procedures issued from time to time in order to ensure audit compliance.

2.5.4 System

a) The RA shall provide all hardware and operating software as per specification determined by POS DIGICERT. The cost of which will be borne by the appointed RA.

b) Any upgrading costs to the system will also be borne by the RA.

2.5.5 Location

a) The RA will identify the location taking into consideration the geographical aspect and supply the relevant furniture and fittings to the specification approved by POS DIGICERT. The RA has to ensure network connectivity is in place and ready for operation.

b) The RA is to ensure the location is adequately secured and covered by insurance policy.

2.5.6 CMS Client Software.

POS DIGICERT shall charge the cost of the software to the RA.

2.5.7 Testing and commissioning

a) POS DIGICERT and RA will jointly conduct testing and commissioning.

b) Trail run operating method will also be conducted jointly.

3) PERFORMANCE BOND

An RA shall provide a performance bond amounting to a minimum of RM25,000.00 in a form of bank guarantee to POS DIGICERT to ensure the RA complies with and is committed to the Standard Operating Procedures (SOP) of RA. Notwithstanding the above, POS DIGICERT shall always reserve its right to set the amount of the performance bond on a case to case basis.

4) LEGAL MATTERS

An RA shall enter into the RA Agreement with POS DIGICERT upon appointment as RA. The agreement will be reviewed upon renewal of the agreement. Each party shall bear its own legal or other professional costs and expenses incurred in the preparation of this agreement.

5) ANNUAL REVIEW

5.1 Each RA shall be audited by the CA on an annual basis as per the requirement under regulation 41 of the DSR 1998.

5.2 The Chief Operating Officer (COO) of POS DIGICERT shall review the results of the audit in order to ascertain as to whether the RA shall be allowed to continue to operate under POS DIGICERT.

5.3 A finding of non-compliance to DSA/ DSR shall be the grounds for dismissing the RA from operating under POS DIGICERT.

5.4 POS DIGICERT shall also actively encourage the RA to develop policies, procedures and other such documentation for its processes. Where such documents already exist, POS DIGICERT shall encourage the RA to keep the documentation up-to-date at all times. These documents shall be referred during audit exercise.

5.5 In addition to this requirement, POS DIGICERT may send its personnel to the RA's premises for an independent review of the RA operation.

5.6 Shall the RA refuse to be inspected either by the qualified auditor and/or POS DIGICERT's personnel; this may be a potential ground for dismissing the RA from operating under POS DIGICERT.

6) RECORD KEEPING

6.1 The RA shall keep and maintain detailed written records documenting -

a) the security measures taken to comply with the DSA/DSR; i.e. if the records kept in digital form it shall be digitally signed.

b) if the RA generates a key pair for a subscriber, the relevant time at which and the manner in which the private key is distributed or transmitted to the subscriber;
c) the relevant time at which and the manner in which a certificate is issued and distributed or transmitted to the subscriber;
d) the certificates issued by it in such a way that the data and its unfalsified condition may be verified at any time; and
e) all other measures taken to comply with the DSA/DSR.

6.2 The records required in section 6.1 shall include evidence demonstrating that the RA has -

a) confirmed the identification of the person named in a certificate that the RA has issued
b) confirmed the identification of the person requesting for revocation of each certificate that the RA has revoked;
c) confirmed all other facts listed as confirmed in a certificate that the RA has issued; and
d) complied with the DSA/DSR in issuing, publishing, suspending and revoking a certificate.

6.3 The RA may require a subscriber or the agent of a subscriber to submit documentation and other evidence reasonably sufficient to enable the RA to comply with the DSA/DSR.

6.4 The RA shall retain all its record of application processing, acceptance and any suspension or revocation of a certificate for not less than ten years from the date of last entry or the date of issue, as the case may be.

6.5 The RA shall keep its records in a secure place and in a secure manner.

7) TERMINATION OF RA

7.1 POS DIGICERT or the Commission have the option to terminate an RA by giving thirty (30) days prior notice.

7.2 The termination of RA shall not affect the validity or effect of any certificate issued by the RA concerned before such termination.

7.3 Upon termination of RA, an official Notice of Termination *(refer Appendix 2)* shall be issued to the affected RA. RP and RO certificates shall be revoked immediately after the 30 days' notice period. At this juncture the respective RA would not be able to issue anymore certificates.

7.4 The affected RA is required to prepare all handover documents and conduct a briefing within 14 days of receiving the termination notice.

7.5 Among (but not limited to) documents to be prepared:

a) List of active certificates
b) Inventory of records (stock & inventory)
c) Up-to-date Standard Operating Procedure
d) Hard copies of all end user information / credentials including back

logs / pending requests + supporting documents.

7.6 POS DIGICERT shall appoint its internal RA and/or another RA to take over the certificates issued by the RA whose contract has been terminated or has expired and such certificates shall, to the extent that they comply with the requirements of the Licensed CA, be deemed to have been issued by that Licensed CA.

7.7 POS DIGICERT shall ensure that all related records and documents are kept in a secure and safe place for up to ten (10) years.

7.8 POS DIGICERT shall notify all affected subscribers and its relying parties on the RA termination via:

7.8.1 Notification on CA's website

7.8.2 Any other publication methods accessible by subscribers

(THIS PART IS INTENTIONALLY LEFT BLANK)

Appendix 1 – Letter of Authorization on Appointment of RA Manager / RO / RP

[RA LETTER HEAD]

[Date]

CHIEF OPERATING OFFICER
POS DIGICERT SDN BHD
8-3A-02, Star Central,
Lingkaran Cyberpoint Timur,
63000 Cyberjaya, Selangor Darul Ehsan

Dear Sir/ Madam,

APPOINTMENT OF REGISTRATION AUTHORITY (RA) MANAGER / OFFICER / PERSONNEL

I hereby appoint the below employee as the **Registration Authority (RA) Manager / Registration Officer (RO) / Registration Personnel (RP)** (underline which is applicable) for [RA company name]. He/she has been servicing [RA company name] for [no of years]. [RA company name] has conducted a background check on him/her against any criminal or fraudulent history and did not find any such record.

Name	:	
NRIC	:	
Staff ID	:	
Designation	:	
Department/Division	:	

Thank you.

Yours faithfully,
[SIGNATURE]

_____

[NAME]
[NRIC]
[DESIGNATION]

RA Company Stamp

Appendix 2 – Notice of Termination of a Registration Authority (RA)

[Date]
CHIEF OPERATING OFFICER
POS DIGICERT SDN BHD
8-3A-02, Star Central,
Lingkaran Cyberpoint Timur,
63000 Cyberjaya, Selangor Darul Ehsan

RA MANAGER
[RA Company Name]
[RA Company Address]
[RA Company Address]
[RA Company Address]
Dear Sir/ Madam,
NOTICE OF TERMINATION OF A REGISTRATION AUTHORITY (RA)

[Contents will depend on the actual reasons of termination]

Thank you.

Yours faithfully,
POS DIGICERT SDN BHD
[SIGNATURE]

_____
[NAME]
[Chief Operating Officer]