Myanmar Online Security Service Certification Authority (MOSS CA)

ouaocvurwr0g'

(Certificate Policy)

aep/ 2012 cEp ! {|yv (1) &u/

rmwum

1. e'ge; (Introduction)

þpmwr;on Myanmar Online Security Service Co., Ltd. \ Myanmar Online Security Service Certification Authority (MOSS CA) r ouaocvurwxway;yici&o tjzpaqmi&u &mwi ouaocvurwxway;jci;qi&mr0g'rsm; (Certificate Policies (CP)) u azmjya&;om;xm; aom pmwr;jzpygon/ þpmwr;wi MOSS CA r ouaocvurwim;&r;o;porsm; (Subscribers) o 'p*spw,ouaocvurwrsm;xway;jci; ? ouwr;w;jci; ? prcecjci; ? y,zsujci;rsm; jylvy&mwi vuemusio;rn MOSS CA \ ouaocvurwxway;jci;qi&mr0g'rsm;u azmjy xm;ygon/ ,i;tjyi MOSS CA Ei ouqiyg0iorsm;tm;v;twu ouaocvurwEi qiaom p;ym;a&; ? 0ya'a&;&m Ei en;ynmyi;qi&mrsm; ? ,lunpwcsrqi&m 0eaqmirrsm; (Trust Services) ? axmuyay;jci;qi&mrsm;uvn; azmjyxm;ygon/

þ CP on Internet Engineering Task Force (IETF) RFC 3647 \ Certificate Policies (CP) Ei Certificate Practice Statement (CPS) a&;q&rn vr;necsursm;twi; a&;qxm;jci; jzpygon/ þ CP wi o;pxm;aompum;v;rsm;\ t"yg,owrwcsursm;on tvuxa&mepquo,aqmi&u a&;0ya' (Electronic Transactions Law) ? ,i;Eiouqiaom en;0ya'rsm; ? trealujimpmrsm; twi; jzpygon/

þ CP on MOSS CA \ ouaocvurwEiqiaom 0eaqmirrsm;twuom to;0iyg on/

1.1 tcsutvutus0;csy (Overview)

Myanmar Online Security Service Co., Ltd. tm; ouaocvurwxway;yici&o (MOSS CA) tjzp vyie;aqmi&uEi&e jynaxmipjrermEiiawmtp;& ? quo,a&; ? pmwuEi alu;ee; 0elu;Xme ? quo,a&;nelum;r0;p;Xme \ 2010 cEp ? E0ibmv 1 &u aepyg pmtrw 327-qn^c(2)a&;^CA^1830 jzi vyie;vyuici vipi&&cygon/ MOSS CA on ouaoc vurwim;&r;o;prnorsm;twu 'p*spw,ouaocvurwrsm; (Digital Certificates) u vurwa&;x;xway;ygon/ ,i;tjyi Certificate Life Cycle 0eaqmirrsm; (ouaocvurw topxway;jci; ? ouwr;w;jci; ? prcecjci; ? y,zsujci;) tm;v;uvn; aqmi&uay;ygon/ MOSS CA \ ouaocvurwu Root CA r vurwa&;x;xway;ygon/ þ CP wi ouaocvurwo;porsm;twu aqmi&uxm;rrsm; ? MOSS CA r ouaocvurw xway; &mwi vuemusio;rn en;vr;rsm;Ei ouaocvurwrwwr;wu aqmi&uxm;rrsm; yg0ijy; 4i;u www.moss.com.mm wi Download jylvy&,Eiygon/

rwywicivyay;yici&o (Registration Authorities, RAs) rsm;on ouaocvurw awmi;qav|muxm;jci;rsm;twu ppreaumi;Ei reueaumi; ppaq;jci;rsm;u jy|vyygon/

ouaocvurw\ trd;tpm;Ei to;jy|ytvu im;&r;o;por 'p*spw, ouaoc vurwrsm;u Servers \wn&ruouaoc&etwuvn;aumi;? Code Ei Content rsm; vurw a&;x;&mwivn;aumi;? pm&upmwr;rsm;wi '*spw, vurwa&;x;í ay;y&mwi vjcr&ap&e Ei ay;yoreueaumi;tcsutvu rsm;\ reueruo&Eiap&evn;aumi; to;jy|Eiygon/

1.2 CP trnEi trwtom; (Document Name and Identification)

þpmwr;on MOSS CA \ CP jzpygon/ þ CP \ Object Identification Value (OID) rm (2.16.104.1.1.2.3) jzpygon/ þ OID u r0g'rsm;xyrowrw&e v tyygu w;cs|Eiygon/

1.3 PKI wiyg0iorsm; (PKI Participants)

1.3.1 A[tz

þ CP wi azmjyxm;aom A[tzon tvuxa&mep quo, aqmi&ua&;0ya' t& zpn;xm;aom tvuxa&mep quo, aqmi&ua&; A[tz jzpygon/

1.3.2 lu;luyrtz

þ CP wi azmjyxm;aom lu;luyrtzon tvuxa&mep quo, aqmi&ua&;0ya' t& zpn;xm;aom tvuxa&mep quo, aqmi&ua&; lu;luyrtz jzpygon/

1.3.3 rvt&i;tjrp ouaocvurw xway;yici&o (Root Certification Authority)

Root Certification Authority (Root CA) on tvuxa&mep quo, aqmi&ua&; lu;luyrtzu en;ynmqi&mtaxmutuay;&e? ouaocvurw xway;yici&o (CA) rsm; o ouaocvurwrsm; xway;jci;? ouwr;w;jci;? prcecjci;? y, zsujci;rsm; jy|vyEi&e twu tvuxa&mep quo, aqmi&ua&; 0ya' t& lu;luyrtzu trepmjzi wm0eay; ce tyxm;aom tztpn;jzpygon/ jrermowi;tcsutvuEien;ynmaumya&;&i;vrwur Root CA tjzp vyuivsu&ygon/

1.3.4 ouaocvurwxway;yici&o (Certification Authority (CA))

Myanmar Online Security Service Co., Ltd. on ouaocvurwxway;yici&o tjzp 'p*spw, ouaocvurwEiqiaom 0eaqmirrsm; ay;vsu&ygon/ MOSS CA \ ouaoc

vurwu Root CA r vurwa&;x; xway;yg on/ im;&r;o;po (Subscriber) rsm;twu ouaocvurwu MOSS CA r pppxway;yg on/

Myanmar Online Security Service Co., Ltd. on tvuxa&mepquo,aqmi&ua&; A[tz\ci jy c u jzi lu;luyrtzr xway;xm;aom CA vyie;vipi &&xm;aom tztpn; jzpyg on/

1.3.5 ouaocvurw im;&r;o;porsm; (Subscribers)

MOSS CA rxway;aom ouaocvurwuim;&r;o;pot m; ouaocvurwim;&r;o;po (Subscriber) rsm;[ac:qyg on/ ouaocvurw im;&r;o;po (Subscriber) rsm;on vwp0;csi;aomvn;aumi;? tz tpn; aomvn;aumi;? en;ynmqi&m ypn;rsm;aom vn;aumi; jzpEiyg on/

1.3.6 ouaocvurwu,lunpwcpmvuct o;jyorsm; (Relying Parties)

MOSS CA r xway;aomouaocvurwrsm;u ,lunpwcpm vuco;paomorsm;on Relying Party rsm;jzpyg on/

xorsm;rm -

1/ MOSS CA Ei Cross-Certification jyvyxm;on Foreign CA rsm;?

2/ MOSS CA Ei Cross-Certification jyvyxm;on Foreign CA rsm; \ ouaocvurw im;&r;o;porsm;?

3/ MOSS CA r xwjyexm;aomouaocvurwy,zupm&i; (CRL) rsm;? ouaocvurwim;&r;o;porsm;\ 'p*spw,vurw (Digital Sign) uvuc to;jyorsm;/

1.3.7 rwywici vyay;yici&o (Registration Authority (RA))

rwywici vyay;yici&o (RA) qonrm ouaocvurw avmuxm;o\ talumi; t&mrsm;Ei ywouí vucaqmi&urwwr;wijci; (Registration) ? avmuxm;otrewu, [w ? r[w ppaq;jci; (Identification) Ei avmuxm;otm; ouaocrppaq;jci; (Authentication) wtwu wm0e,aqmi&uay;aom vy*v (or[w) tztpn;wpc jzpyg on/ (qvonrm RA on CA u,pm; reuer& ? r& ppaq;jci; (Identification) Ei ouaocrppaq;jci; (Authentication) wm0ersm;u aqmi&uay;yg on/)

1.3.8 ouaocvurw rwwr;wu (Repository of Digital Certificates)

ouaocvurw rwwr;wuqonrm MOSSCA r xway;xm;aom ouaocvurw rsm;Ei ouaocvurwy,zupm&i;rsm;tm;v;u trsm;jynor tcera&;0ia&mulun&Ei&e or;qn; rwwr;wixm;on MOSSCA \ouaocvurw rwwr;wujzpygon/ xrwwr; wuu (24) em& ? (7) &uywv; (Internet quo,rjywawmuaecerví) 0ia&mulun&Eiatmi praqmi&uxm;ygon/

1.3.9 CP oiawmto;0ir (Applicability)

þ CP & vyx;vyen;rsm;?vuemuio;rnen;vr;rsm; (Practices) tm;v;on jrerm Eiitwi;wi MOSS CA r ouaocvurw im;&r;o;porsm;o xway;xm;on ouaoc vurwEi ouaocvurwy,zupm&i; (Certificate Revocation List (CRL)) rsm;u to;jyjci; rsm;?ouaocvurwouwr;w;jci;rsm; tm;v;Ei ouqitus;0iygon/

1.4 ouaocvurw to;jyr (Certificate Usage)

1.4.1 ouaocvurwu oiawmaom to;csr (Appropriate Certificate Usage)

MOSS CA r ouaocvurw im;&r;o;porsm;o xway;aom ouaocvurwrsm;u –

- 'p*spw,vurwa&;x;&e (Sign)?
- E-mail u v0uu'ajymi;íay;yEi&e (Encrypt)?
- ay;yaom tcutvursm;ur&i;pmtwi; ajymi;vzw&&e (Decrypt)?
- E-mail ay;yo rnorn0gpprealumi; taxmutxm;tjzpto;jy&e (Prove Identity)?
- Code Signing jyvvy&e Ei
- Services rsm;u Authenticate (Client/ServerAuthentication) jyvvy&e

wtwu to;jyEiygon/

Relying Party r,lunpwcsí,i;&n&,csursm;tjyi tjcm;aom &n&,csursm;twu ouaocvurwu to;jyvygu wnq0ya'rsm;?þ CP ? CPS wEi uunr&vi to;jyEiygon/ouaocvurwtrs; tpm;tm;jzi atmuygtwi; o;rs;&ygon/

Certificate Class	Assurance Level			Usage				
	Low	Medium	High	Signing	encryption	Client Authentication	code/ content signing	Secure SSL/ TLS sessions
Class-1 Certificate	Â			Â	Â	Â		
Class-2 Certificate		Â		Â	Â	Â		
Class-3 Certificate (Individual)			Â	Â	Â	Â	Â	
Class-3 Certificate (Organization)			Â	Â	Â	Â	Â	Â

Table (1)- Individual/Organization Certificate Usage.

Class 1 Certificate

Class 1 trsm;tpm; ouaocvurwon vu,wivma&mu avsmuxm;&ervb e-mail **jzi** Online **avsmuxm;orsm;u xway;aom ouaocvurw trsm;tpm; jzpygon/**

Class 2 Certificate

Class 2 trsm;tpm;ouaocvurwu avsmuxm;or vtyaom taxmutxm;pm&upmwr;rsm; Eiwu avsmuxm;&rnjzpygon/ vu,wivma&muavmuxm;&ervyg/

Class 3 Certificate

Class 3 trsm;tpm; ouaocvurwu avsmuxm;or vtyaom taxmutxm; pm&upmwr; rsm;Ei avmuxm;ou,wir vma&mu avsmuxm;jci; ? xw,jci; jymvy&ygrn/ vtyaom taxmutxm;rsm;witen;q;taejzi atmuygwyg0i&rn/

(1) rwywir&i;Ei rwl ?

(2) oe;acgipm&i;r&i;Ei rwl ?

(3) &pce;Ei&yuuaxmucpm

(4) tztpn;rsm;jzpygu

- **tztpn;/urP\ rwywir&i;? rwl**
- **tztpn;rw&m;0iu,pm;v,vpm** (Authorization Letter)

wjzpygon/

1.4.1.1 Assurance Levels

Low Assurance Level : ,lunpwc&rtqieraom ouaocvurwtr;tpm;jzpygon/ xouaocvurwtm; Authentication jyvy&eEi Non-Repudiation uaxmuyay;&e &n&,cu rsm;jzito;rjyoiyg/ þouaocvurwon im;&r;o;po\u,a&;tcutvursm; (Identity) u ouaoc&mwi to;rjyEiyg/ Relying Party r im;&r;o;po\ ouaocvurwu to;jyí tcutvursm;u v0uuwtjzp ajymi;vEiaomvn; vucoon ouaocvurwyiqio pprealumi;aocmr r&Eiyg/

Medium Assurance Level : ,lunpwc&rtv,tvwtqi (Medium) &aom ouaoc vurw tr;tpm;jzpygon/ þouaocvurwu tztpn;twi;Ei p;ym;a&;qi&mrsm; ? t;ar;vto;jyrwi im;&r;o;po\ u,a&;tcutvursm; (Identity) u ouaoc&m wi ,lunpwc&rtv,tvwtqi (Medium) vtyaomtcg to;jy&eoiavsmygon/

High Assurance Level : ,lunpwc&r tqijriaom ouaocvurwtr;tpm;jzpygon/ im;&r;o;po\ u,a&;tcutvursm; (Identity) u ouaoc&mwi ,lunpwc&rtqirm ouaocvurw tr;tpm; Class 1 Ei Class 2 xuyí jriygon/

1.4.2 wm;jrpxm;on ouaocvurw to;jyrrsm; (Prohibited Certificate Uses)

tvuxa&mep quo,aqmi&ua&;0ya' ? ,i;Eiouqion en;0ya'rsm;Ei tre alumjimpmrsm;wi cijyxm;ontwi; ? ouaocvurwwi cijyxm;aomcijyctut&om ouaocvurwrsm;u to;jy&rn/ vuxcu'gP&m &apEiaom ? aoq;apEiaom (o) obm0yw0e;uiu xcuysup;apon pepsm;\ xe;cyr u&,mrsm;wi ouaocvurwu xe;cy&e&n&,cujzito;rjy&yg/ MOSS CA \ ouaocvurwu im;&r;o;porsm; (Subscriber) o 'p*spw,ouaocvurw xway;jci; ? CRL Sign x;ci;pon CA vyie;rsm;rví tjcm;aomaqmi&urrsm;twu to;rjy&yg/ Subscriber twu xway;aom ouaocvurwu CA Certificate tjzp to;rjy&yg/ Class-1 Certificate rsm;u ouaocvurw uiaqmio\ wn&rouao jy&e (Proof of Identity) Ei aqmi&urrsm;u jii;qjci;rjyvyEi&e (non repudiation) &n&,cursm;twu to;rjy&yg/

1.5 ouaocvurwxway;jci;qi&mr0g'rsm; prcecjci; (Policy Administration)

1.5.1 CP/CPS tm; pr?tycsya&;qi&m tztpn; (Organization Administering the Document)

Address - Myanmar Online Security Service Co., Ltd.,
Building (17), Ground Floor,MICT Park,
Universities' Hlaing Campus, Hlaing Township,
Yangon, Union of Myanmar
http://www.moss.com.mm

Attention- Department Head

Phone - (95)-1-521128

Fax - (95)-1-521129

E-Mail - operation@moss.com.mm

1.5.2 quo,&rno (Contact Person)

Department Head
Myanmar Online Security Service Certification Authority
Myanmar Online Security Service Co., Ltd.

1.5.3 CP/CPS \oiavsmruq;jzway;rno

(Person Determining CP/CPS Suitability for the Policy)

lu;luyrtzEi Root CA on þ CP Ei CPS \ oiavsmrEi to;0iru q;jzwygon/

1.5.4 CP/CPS uvucrnvyx;vyen;rsm; (CP/CPS Approval Procedure)

þ CP u A[tz\ oabmwncsujzi lu;luyrtzr twnjyjy;jzpygon/ CP/CPS u jyiqicsursm; (Amendments) &vli lu;luyrtzowijy ? twnjycsu&,jy; MOSS CA r jyiqijci; jyvyEiygon/ jyiqion Version Ei jyiqirrsm; (Updates) u MOSS CA \ WebSite & http://www.moss.com.mm wiazmjyxm;ygon/ jyiqirrsm;on 4i; CP \ e*rv ReferenceVersion & &n&,xm;on (Designated) (o) qeusirrsm; (Conflicts) u ae&m,^vr;r;r &ygon/ þ CP wi jyiqiralumi CP Eiouqiaom Object Identifier wi jyiqi&e v tyygu Root CA xwijyjy; cijycsujzi aqmi&uygon/

1.6 t"yg,owrwcsuEi twausupmv;rsm; (Definitions and Acronyms)

aemuquw(u) Z,m;Ei aemuquw(c)wi azmjyxm;ygon/

2. yEyxwa0jci;Ei ouaocvurwrwwr;wu\ wm0ersm;

(Publication and Repository Responsibilities)

2.1 ouaocvurw rwwr;wu (Repository)

MOSSCAon trsm;jynorouaocvurwrsm;u0ia&mulun&eirn Online ouaoc vurwrwwr;wu (Repository) xm;&ygon/ MOSS CA r xway;xm;aom ouaoc vurwrsm;Ei zsuor;xm;aom ouaocvurwrsm; (CRL) u ,i;rwwr;wuwitrsm;jyno lun&Ei&etvim xwa0azmjyxm;ygon/ xtjyi ouaocvurwu,lunpmvuc to;jylo (Relying Party) r ouaocvurw\ tajctae (Certificate Status) Ei ywouaom tcsu tvursm;u MOSSCA \ Website jzpaom (www.moss.com.mm) wi &mazlun&Ei&e owi;tcsutvursm;u vn; azmjyay;xm;ygon/

2.2 ouaocvurw tcsutvursm;u yEyxwa0jci;

(Publication of Certificate Information)

MOSS CA r xway;xm;aom ouaocvurwrsm;\ tajctae (Certificate Status) ? ouaocvurwy,zsupm&i;rsm; (CRL) Ei ywouaomtajctaersm;u lun&Ei&e ? ouaoc vurwu ,lunpmvucto;jylo (Relying Parties) rsm; Download jylvyEi&e Web-Based ouaocvurwrwwr;wu (Repository) xm;&ygon/ xtjyi OCSP (Online Certificate Status Protocol) 0eaqmir (&ygu) to;jyí Relying Party rsm;r ouaocvurwtm; ppaq;Eirn en;vr;rsm;u azmjyay;xm;ygrn/

MOSS CA on atmuygtcsutvursm;u rnorqlun&Ei&e ,i;\ WebSite http://www.moss.com.mm witcsejyn azmjyxm;ygon/

- MOSS CA \ Certification Practice Statement (CPS) ?
- MOSS CA \ Certificate Policy (CP) ?
- Root CA \ ouaocvurw ?
- MOSS CA \ouaocvurw ?
- MOSS CA r xway;xm;on Subscriber rsm;\ouaocvurwrsm;Ei ouaoc vurwy,zsupm&i;rsm; ?
- MOSS CA \ im;&r;o;porsm; oabmwpmcsy (Subscriber Agreements) ?
- ouaocvurwu,lunpwcspmvucto;jylorsm; oabmwpmcsy (Relying Party Agreements) ?
- ouaocvurwto;jyr User Manual rsm; ?

2.3 yEyxwa0rn t|urEi tc:e (Time or Frequency of Publication)

MOSS CA rxway;x|m;aom ouaocvurwr|sm;Ei ouaocvurwy,z:upm&i; (CRL) r|sm;u ouaocvurwxway;jci; ? y,z:ujci;jy|vyon tc|gwi; Website wi xwjyeay;rn/ tu,í CRL wiaz|mjyx|m;aom ouaocvurwr|m ouwr;ueq;o|m;y|gu xouaocvurw ouwr;ueq;|y;aem|uyi; xwjyex|m;aom CRL r|sm;wi ¤i;u xnoi; vrrn r[wy|g/

2.4 ouaocvurw rwwr;wu& tc:u t vur|sm;xe;c|syr

(Access Controls on Respository)

MOSS CA on ouaocvurw rwwr;wu& tc:u t vu (Data) r|sm;t|m; vyyici r&aom y*|vr|sm;r xyrjznpujci;? z:ujci;? jy|jyijci;r|sm; rjy|vyEi&ev tyaom umu, xe;c|syr tptr (Control) r|sm; jy|vyx|m;y|gon/ ouaocvurw rwwr;wu t|m; 0ia&mu |un&jci;u ueowx|m;jci;r&y|g/ ouaocvurwr|sm;? ouaocvurw tajctaeqi&m tc:u t vur|sm;Ei CRL u0ia&mu|un&Ei&e Relying Party Agreement (RPA) u oab|mwn& rn jzpy|gon/

3. ouaocjci;Eippaq;jci; (Identification and Authentication)

3.1 trnay;jci; (Naming)

3.1.1 trn tr|s;tp|m;r|sm; (Type of Names)

ouaoc vurwi|m;&r;o;por|sm;\ ouaocvurw Subject Name Field wi X.501 Distinguished Name (DN) y|g0iy|gon/ ouaocvurw\ Subject Distinguished Name (DN) wiy|g0iaom Common Name (CN) on Domain Name wpc ? E-Mail Address wpc? tztpn;wpc\ w&m;0itrn jzp&y|grn/ ouaocvurwwiy|g0iaom tztpn; (O) on tztpn;\w&m;0itrnuaz|mjyy|gon/ vy*|vtrnjzi av|muxm;aom ouaocvurw (Individual Certificate) jzpy|gu xo\u,yitrn jzp&rn/

3.1.2 trnr|sm; t"y|g,jyn0ap&ev tyjci; (Need for Name to be Meaningful)

ouaocvurw i|m;&r;o;por|sm;on ouaocvurwr|sm;\ Subject Field wiy|g0irn trnr|sm;u e|m;vn&ev,uon? tr|sm;o&aom &i;vi;aom ? t"y|g,&on4i;w\ wn&ru q;jzwray;&e trnr|sm;u to;jy&rn/

3.1.3 ouaocvurw im;&r;o;po\ trnurm;

(Anonymity or Pseudonymity of Subscribers)

MOSS CA on ouaocvurwim;&r;o;p&e av\muxm;orm;tm;rr (o) tztpn; \ trnrm;u emrn&i; r[won tjcm;aom trnrm; xm;&o;pcirjy\yg/

3.1.4 trnrm;u bmomjyern pn;r0;rm; (Rules for Interpreting Various Name Forms)

jyXme;xm;jci;r&yg/

3.1.5 trnrm;xywrr&jci; (Uniqueness of Names)

ouaocvurw im;&r;o;porm;\ Subject Distinguished Name rm;on MOSS CA \ Domain twi;wi wprs;wn; (Unique) jzp&rn/

3.1.6 totrwjyjci;? ppreaumi;xi&m;apjci;Ei ueypn;trwtom;rm;\ tce;u@

(Recognition, Authentication and Role of Trademarks)

MOSS CA on ouaocvurw av\muxm;orm;tm; tjcm;orm; \ ÓPpr;&nyiqirqi&m tcita&; (Intellectual Property Right (IPR)) uus;verjzpapon trnrm;o;pav\muxm;jci; cirjy\yg/ av\muxm;orm;on tjcm;orm;\ IPR u azmuzsujci; &? r&u MOSS CA r ppaq;jci;rjy\vyyg/ tu,íxotjii;ym;rrm;ay:ayguvmygu MOSS CAon xo\ouaocvurwav\muxm;jci; Ei ouaocvurwwu y,zsuEion (o) qi;ixm;yici&on/

3.2 ue0; rnorn0gjzpaumi; ppaq;jci; (Initial Identity Validation)

3.2.1 Private Key yiqiaumi;ouaojyrnen;vr;

(Method to Prove Possession of Private Key)

ouaocvurwav\muxm;oon ouaocvurwxw&mwi to;jy\rn Private Key on ¤i;yiqijci; reueaumi; ouaojy&rn/ xoouaojy&mwi PKCS#10 File (o) tjcm; aom ,i;uoaom Cyrptographic en;vr;rm; (o) MOSS CA r oabmwxm;onen;vr;rm;jzi ouaojyEiygon/ MOSS CA r im;&r;o;pou,pm; Key rm; Generate jy\vyay;ygu þv tycsuon tus;r0iyg? rouqiyg/

3.2.2 tz\tpn; pprer&alumi; xi&m;ap&eppaq;jci;

(Authentication of Organization Identity)

ouaocvurwwi tztpn;trnrsm;yg0iontcgwi;wi xtztpn; trewu, wn&rEi ouaocvurwav\muxm;oray;aom av\muxm;ryg tjcm;tcursm; (ppaq;&e rv tyon tcursm;rví) reuer&alumi;u MOSS CA \ rwywijci;qi&mvyie;rsm;aqmi&u aom tztpn; (RA) r Document ppaq;on en;vr;rsm;twi;ppaq; twnjy\yg on/ RA on ouaocvurwav\muxm;otm; ppaq;&mwi terq;tqitm;jzi -

- tztpn;trewu,wn&alumi;u tp;&tztpn;r xway;xm;on tztpn;qi&m pm&upmwr;rsm; (o) tztpn;wn&rutmrcEiontmPmyitztpn;wpcc\ pm&u pmwr;? axmuccursm;u ppaq;jci;rsm; jy\vyygon/
- ouaocvurwav\muxm;otm;,i;\tztpn;rcijy\cujzi av\muxm;jci;jzpalumi;? tztpn;r o&alumi;u w,vze; (o) pm (o) tjcm;aom en;vr;rsm;uo;í ppaq; twnjy\yg on/ ouaocvurwwi y*\vwp0;0;\ trnon tztpn;\u,pm;v, taejzi yg0iontcg xoon ,i;tztpn;\ 0exr; [w ? r[wEi tztpn; u,pm; vyyici &? r& wu MOSS CA Ei RA r ppaq;ygon/
- ouaocvurwwi Domain Name (o) E-mail Domain rsm;yg0iygu ouaocvurw av\muxm;oon x Domain Name (o) E-mail Domain Name uo;pci &? r& wu ppaq; rn jzpygon/

jrermEiitp;&r jyXme;xm;aom 0ya'rsm;? ouqionen;0ya'rsm;? trealumjimpmrsm;? vipipm&upmwr;rsm;Ei vyx;vyen;rsm;twi; tjcm;aom ppaq;rrsm;u vtyygu jy\vy om;rn jzpygon/

3.2.3 wp0;ci;p\ wn&ru ppaq;jci; (Authentication of Identity)

ouaocvurwav\muxm;o wp0;wpa,mucsi;p\ Identity ppaq;jci;u ouaoc vurw trs;tpm;tvu jy\vyygrn/ av\muxm;ou terq;tm;jzi Eiiom;pppa&;u'jym; (o) rwywiu' (o) Eiiu;vurwEi wuqippaq;jci;rsm; jy\vyygrn/

ouaocvurwim;&r;o;potm;ppaq;jci;jy\vyrntcursm; (Authentication Standard) u ouaocvurw trs;tpm;tvu atmuyg Z,m;wi azmjyxm;ygon/

ouaocvu rwtr&;tpm;	ppaq;rnen;vr;
Class – 1	ppaq;r rjy|vyy/ oaom ouaocvurwav|muxm;o\ E-mail Address jzi jye|um;c&u (Reply Mail) vuc&&rom ouaocvurw xway;yg on/
Class - 2	ouaocvurw av|muxm;or ay;aom tc&utvur&m;u CA (o) RA r vucaom rwwr;r&m; (Database) or;qn;xm;on tztpn;r&m;(o) p;ym;a&; qi&mrwwr;r&m;? vr;nepm tyr&m;? 0exr;pm&i;r&m;^rwwr;r&m; (o) Database r&m;& tc&utvur&m;Ei wuqippaq;jci;r&m; jy|vyyg on/
Class - 3	Class-3 Certificate ppaq;jci;u av|muxm;ou ,wi RA a&armuovu ,wi vma&muapjci;jzi ppaq;yg on/ av|muxm;ou Eiiom;pppa&;u'jym; (o) rwy wiu'&"gwy(o) Eiiu;vurw& "gwyEi wuqippaq;jci; r&m; jy|vyyg on/

Table (2)-Authentication of Individual Identity

3.2.4 tc&i;c&i;vyie;vyaqmiEir&&etwu ourwc&ur&m;

(Criteria For Interoperation)

jyXme;xm;jci;r&yg/

3.3 ouwr;w;&eav|muxm;rr&m;u reuer&? r& ppaq;jci;Ei ouaocrppaq;jci;

(Identification and Authentication for Re-Key Request)

'p*&pw ,ouaocvurwr&m;ouwr;rueq;rouaocvurwto;jy|ci; jywawmur r&ap&etwu ouaocvurw topwpc &&&evtyyg on/ ouaocvurwr&m;tm;v; ouwr;w;on tcg ty' (4.2) twi;ppaq;í ouwr;ueq;rnouaocvurw\ ae&mwi tpm; x;&etwu ouaocvurwtopwpcu MOSS CA r xway;yg on/

3.3.1 yreouwr;w; (Re-Key) r&m;uppaq;jci;Ei twnjy|ci;

(Identification and Authentication for Routine Re-Key)

ouaocvurw ouwr;w;jci; (Re-Key) rjy|vyr Re-Key av|muxm;jci;jy|vyo vy*|v (o) tztpn;on xouaocvurwuiaqmio (Subscriber) tpptrejzpa|umi; ty' (4.6) yg owrwc&ur&m;twi;ppaq;yg on/

ouaocvurw tr&;tpm; (Class 1) twu ouwr;w;jci; vucrnen;vr;wpcrm Challenge Phrase (o) tvm;wwpcc (o) Private Key yiqia|umi;ouaojy|ci;w|zi

ouwr;w;av|mux|m;jci;u vucjci;jzpygon/ ouaocvurwouwr;w;jci; aqmi&u&m wi ouwr;w;av|mux|m;oon 4i;\ Challenge Phrase (o) tvm;wu reuepm jznpuay;Ei ? ajymEiontjyiouwr;w;av|mu&mwi jznoi;ontcsursm;Ei ue0; ouaocvurw av|mux|m;&mwi jznoi;ontcsutvursm; (aumy&w Ei Technical Contact Information rsm; tygt0i) ujym;r ? ajymi;vrr&ygu ouwr;w;ouaocvurwtopu xway;rnjzpygon/

Rekey (o) Renewal jy|vy&eawmi;qontcgwi; MOSS CA on ouaocvurw im;&r;o;po av|mux|m;p0u to;jy|on ppaq;onen;vr;rsm; ? ouaocrppaq;jci; jy|vyon en;rsm;twi; jyevnppaq;ygon/

3.3.2 ouaocvurwy,zsuly;aemu ouwr;w; (Re-Key) jy|vy&e av|mux|m;jci; rsm;u ppreal|umi;ppaq;jci;Ei reueal|umi;twnjy|ci;

(Identification and Authentication for Re-Key After Revocation)

atmuazmjyygtal|umi;rsm;al|umi ouaocvurwuy,zsuc&ly;aemu ouwr;w; (Re-Key Ei Renewal) jy|vy&e av|mux|m;vmjci;rsm;u cijy|rnr[wyg/

- ouaocvurwrsm; (Class-1 Certificate rvÍ) MOSS CA (o) RA \ w&m;0icijy|csur&&y ouaocvurw xway;xm;jci;al|umi y,zsuc&c v|i ?
- ouaocvurwav|mux|m;o\ vurwav|mux|m;jci;qi&mtcsursm;u twn jy|ay;or av|mux|m;csuyg tcsursm;on rm;,i;azmjyon (o) rm;,i;aeal|umi; us;al|umi;civpm o&Í ouaocvurwy,zsuc&cv|i ?
- MOSS CA Ei ,i;\vyie;rsm;u umu,apmia&mu&etwu tjcm;aomtal|umi; jycsuuprsm;al|umi y,zsujci;c&cv|i ?

3.4 ouaocvurwy,zsu&eawmi;qjci;twu ppaq;jci;Ei twnjy|ci;

(Identification and Authentication for Revocation Request)

rnonouaocvurwurq y,zsujci;rjy|r MOSS CA Ei ouaocvurw av|mu xm;ou,wir y,zsu&eawmi;qjci;rsm;u aocsmpmppaq;Í q;jzwygon/ ouaocvurw uiaqmior y,zsuay;&e awmi;q ? av|mux|m;jci;rsm;u ppaq;twnjy|aom (Authentication) vyx;vyen;rsm;wi atmuygtcsursm;yg0ion/

- wpcsWaomouaocvurwtrs;tpm;rsm;wi y,zsu&eav|mux|m;oon ouaocvu rw uiaqmio\ Challenge Phrase v|W0upum;p (o) tvm;wpum;pjzi av|mux|m;y;

xpum;pon rwwr;xe;or;xm;aompum;pEiwnv\i ouaocvurwu y,zuay;jci;?

- im;&r;o;por ouaocvurwy,zu&e (Revoke) awmi;qon av\muvmu 4i;r 'p*spw,vurwa&;x;í av\muxm;y; x'p*spw,w,vurwonvn; reuev\i y,zuay;jci;?
- ouaocvurwav\muxm;ox quo,talumi;lum;í y,zu&eawmi;qoon ouaocvurwuiaqmiou,wi jzpalumi;aocsmapjci;? (xoquo,&mwitajc taeay:wirwní Phone? Fax? E-mail? Courier Service rsm;uto;jy\Eiygon)/

MOSS CA \ RA rsm;r Revocation Request rsm; ay;y&mwi RA Administrator r vurwa&;x;í y,zuay;&e awmi;q&rn/

4. ouaocvurw Life-Cycle vyie;aqmi&ur v tycsursm;

(Certificate Life-Cycle Operational Requirements)

4.1 ouaocvurw av\muxm;jci; (Certificate Application)

ouaocvurwo;p&eav\muxm;vygu tce; 204? Myanmar Info-Tech? wuovrsm;vie,ajr?&euejrW& MOSS Sale Office RA xo quo,av\muxm;Eiygon/ av\muvmypu MOSS CA \ Website jzpaom www.moss.com.mm wi Download jy\vyí jznpuav\muxm;Eiygon/

4.1.1 ouaocvurwav\muxm;Eiorsm; (Who Can Submit a Certificate Application?)

- ouaocvurwav\muxm;ou,wi?
- urP? tztpn;trnjzi av\muxm;ygu w&m;0irwywixm;aomurP? tztpn;\ w&m;0iu,pm;v, (Any Authorized Representative)
- MOSS CA \ w&m;0iu,pm;v,rsm;/
- RA \ w&m;0iu,pm;v,rsm;/

4.1.2 pm&i;ay;oi;jci;vyie;Ei vyie;wm0e,rrsm;

(Enrollment Process and Responsibilities)

av\muxm;otm;v;on pm&i;ay;oi;jci;vyie; (Enrollment) wiyg0iaom Certificate Application tm; a&;om;jznpu&mwi reueaom? ppreaom tcsutvursm;jzi jznpuay;&rn/ ouaocvurw av\muxm;otm;v;on ouaocvurw im;&r;o;po oabmwncsu (Subscriber Agreement) wi yg0iaomtcsursm;? tmrccsursm;u oabmwnr&&rn/

ouaocvurwav|muxm;or Key Pair (Public Key Ei Private Key) u rrbmom jy|vyyguu

(u) CA (o) RA xo 4i;w\ Public Key tm;ay;yjci;? (Certificate Signing Request File (PKCS #10)) ay;yjci;?

(c) CA (o) RA xo Public Key Eiuunr&aom Private Key trewu, yiqia|umi; ouaojyjci;wu vyaqmi&rn/

vtyyguu ouaocvurwav|muxm;ou,pm; MOSS CA (o) RA r Key Pair Generate jy|vyay;jci;u aqmi&uygon/

4.2 ouaocvurwav|muxm;jci;uvucaqmi&ujci;

(Certificate Application Processing)

4.2.1 ppaq;jci;vyie;rsm;uaqmi&ujci;

(Performing Identification and Authentication Functions)

MOSS CA Ei RA rsm;on ouaocvurwav|muxm;orsm;tm; vurwxway;jci; rjy|r tcsutvursm;tm; ppaq;jci;u ty' (3.2) twi;aqmi&uygon/

4.2.2 ouaocvurwav|muxm;jci;u vucjci; (o) jii;y,jci;

(Approval or Rejection of Certificate Applications)

ouaocvurwav|muxm;oon ue0;ppaq;jci; (Initial Identity Validation) u ty' (3.2) twi; jy|vyatmijrií owrwxm;aom aia|u;uay;oi;cv|i MOSS CA (o) RA on av|muxm;otm; ouaocvurwu xway;rnjzpygon/ atmuazmjyyg tcsursm;jzpym;v|i ouaocvurw xway;jci;u MOSS CA (o) RA r jii;y,Eion/

- Initial Identity Validation ppaq;jci;u ratmijricv|i ?
- av|muxm;oon vtyaomaxmucpm? y;wpm&upmwr;rsm;ay;&e ysuuucv|i ?
- ta|umi;lum;pmu owrwtcsetwi; ta&;,aqmi&ujci;? ta|umi;jye|um;jci;r&cv|i?
- owrwxm;aomaia|u;u ay;oi;&e ysuuucv|i ?
- ouaocvurw av|muxm;otm; ouaocvurwxway;jci;on MOSS CA (o) RA twu en;ynmyi;qi&m xcurrsm;Ei MOSS CA (o) RA *Poumxcueion[,qv|i ?

4.2.3 ouaocvurwav|muxm;jci;u vucaqmi&uay;onlumjricte

(Time to Process Certificate Applications)

ouaocvurwav|muvmEitw vtyaom y;wtaxmutxm;rsm; jynppmjznpu wijyjy;ontcterpí MOSS CA (o) RA on ouaocvurw xway;&e aqmi&uygon/ vyie;ly;p;&rntceu tvyvy&u (7) &utwi; owrwxm;ygon/ CA r ouaocvurw xw,Eialumi;u av|muxm;otm; e-mail (o) pmjzi (o) ze;jzi talumi;lum;ygon/ ouaocvurw av|muxm;jci;on jii;y,jci; ? y,zujci;rc&ontcetx av|muxm;jci; wnjron (Active) [owrwygon/

4.3 ouaocvurw xway;jci; (Certificate Issuance)

4.3.1 ouaocvurwxway;p0 MOSS CA r aqmi&urrsm;

(MOSS CA Actions during Certificate Issuance)

MOSS CA on ouaocvurw av|muvmwi yg0iaom tcutvursm;u to;jyí ouaocvurw xway;ygon/ ouaocvurw xwly;aemu MOSS CA (o) RA on av|muxm;ox talumi;lum;ygon/ ouaocvurwtrs|;tpm; (Class 2, Class 3) twu av|muxm;orouaocvurwxw,Eialumi;talumi;lum;pmEitw ouaocvurw u RA x av|muxm;ou,wi vma&muxw,&rn/ ouaocvurwtrs|;tpm; (Class 1) twu Web Site r Download vyíaomvn;aumi; ? vu,wirvma&muEiygu u,pm;xw,Ei&e vn;aumi; pp0xm;ygon/ av|muxm;oon Public Key wpcxuyí ouaocvurw xw ay;&e av|muxm;ygu xway;onouaocvurwta&twut& usoiaiu ay;aqmi&rn jzpygon/ MOSS CA on vurwa&;xjci;vyie; (Signing Operations) rsm;u tp;& &;zi&ursm;wiom jy|vyygon/

4.3.2 MOSS CA r im;&r;o;pox ouaocvurwxw,&e talumi;lum;jci;

(Notifications to Subscriber by the CA of Issuance of Certificates)

MOSS CA r ouaocvurwjy|vyly;alumi; RA o 0;pm talumi;lum;ygon/ RA r ouaocvurw xw,Eily|zpalumi; im;&r;o;pox Phone ? Fax ? E-mail ? Courier Service rsm; (wpcc) u to;jyí talumi;lum;ay;ygon/

4.4 ouaocvurwuvucjci; (Certificate Acceptance)

4.4.1 ouaocvurwu&,vucjci; (Conduct Constituting Certificate Acceptance)

ouaocvurwtm; Download jyvyí &,cvi (o) ouaocvurwyg tcutvu rsm;Ei ouaocvurwon rm;,i;alumi; MOSS CA (o) RA x xway;on&urpí (15) &u twi; ueuupmay;yjci;r&cvi ouaocvurwtm; vucon[owrwygon/

4.4.2 ouaocvurwrsm;tm;xwjyeay;jci; (Publication of Certificate by the CA)

MOSS CA r xway;vuaom ouaocvurwrsm;tm; trsm;jynolun&Ei&e MOSSCA \ouaocvurwrwwr;wu (Repository) wi xwjyealunmay;xm;ygon/ xtjyi RootCA trs;om;ouaocvurwrwwr;wu (National Repository) wivn; xwjyeay;xm;rn jzpyg on/

4.5 Key rsm;Ei ouaocvurwto;jyr (Key Pair and Certificate Usage)

4.5.1 Subscriber CA \ Private Key Ei ouaocvurwto;jyr

(Private Key and Certificate Usage)

ouaocvurwu to;jyloon im;&r;o;porsm;\ oabmwnctu (Subscriber Agreement) Ei þ CP ? CPS wwiyg0ion owrwctursm;twi; vuem&e oabmwnrom ouaocvurwu o;p&rn/ ouaocvurwwi yg0iaom Key Usage Field Extension Ei ouaocvurwtm; to;jyjci;won uunr&&rn/ (0yrm- ouaocvurwwi Digital Signature uvyaqmicirjycvi ouaocvurwu vurwa&;x;&etwu to;jyjci; rjyvy &yg/)

ouaocvurwo;porsm;on rrw\ Private Key rsm;u tcir&aomor to;rjyEi&e umu,aqmi&uxm;&rn/ ouaocvurwouwr;ueq;ly;aemuyi;Ei y,zuly;aemuyi; wi xouaocvurwu quvuto; rjy&yg/

4.5.2 Relying Party r Public Key Ei ouaocvurwto;jyrrsm;

(Relying Party Public Key and Certificate Usage)

Relying Party rsm;onouaocvurwEi ,i;ouaocvurwuto;jyía&;x;xm;aom 'p*spw,vurwu ,lunto;jyjci;jyvy&mwi Relying Party Agreement wia&;om;xm;aom tcutvursm;u oabmwrom vucto;jy&rn/

ouaocvurwwpcay:wi ,luno;pron tajctaetr$;r$;ay:rwní talumi; tu$;oiav$mr &?r& u Relying Party r$m; u,wipO;p$m;? q;jzwívuc&rn/ tu,í tajctaewpcon aemuxytmrccurm;&,oion[,qygu Relying Party on xo,lun o;pjci;jy|vy&etwu vtyaomtmrccurm;u xyr&,&rn jzpygon/

xuoaom ,luno;prr$m; rjy|vyr Relying Party r$m;on atmuygtc$uwu vwvypm o;oyjci; (Assess) jy|vy&rn/

- Certificate wiazmjyay;x$m;aom to;jy|r| &n&,c$ut& ouaocvurwt$m; to; jyjci;rm oiav$mr &?r&?
- þ CP r wm;jrp? ueowx$m;jci;r&aomoiawmon&n&,c$uwpctwu trewu, to;jyjci;[w?r[w?
- ouaocvurwEi,i;ouaocvurwuxway;caom (RootCA, CA) r$m;\ ouaoc vurw tajctaew (Status) uppaq;&rn/ ouaocvurw Chain wiyg0iaom ouaocvurwwpccony,z$ujci;cx$m;&aom ouaocvurwjzpygu Relying Party on xouaocvurwu ,lun&eoiroi Ei y,z$uc&rrm u$;alumi;qav$mr &r&u to;rjy|r ppr;ppaq;&e wm0e&ygon/

MOSS CA Ei RA r$m;on ouaocvurw to;jyjci;\ oiav$mr &?r&u ppaq;&e wm0er&y/ ouaocvurwo;pron oiav$mon[,qv|i Relying Party r$m;on oiav$m on Software Ei (o) Hardware uto;jy|í'p*$pw,vurw (Digital Signature) reuealumi; ppaq;r (Digital Signature Verification) u jy|vyjci;aomvn;aumi;?tjc$m;aom Cryptographic Operation uto;jy|íaomvn;aumi; ouaocvurw\ reueruppaq;&rn/ þuo ppaq; aqmi&urr$m;Ei ouaocvurwtay:wi ,luno;prwon qupyygon/ xuo jy|vy ppaq;aqmi&ujci;wi Certificate Chain wpcowrwjci;Ei ,i; Chain wiyg0iaom ouaoc vurwt$m;v;\ Digital Signature r$m; reuealumi; ppaq;jci;wvn;yg0iygon/

4.6 ouaocvurw ouwr;w;jci; (Certificate Renewal)

Certificate Renewal on vu& Key Pair t$m;to;jy|y; ouaocvurw ouwr;w; av|muxmjci;r$;jzpygon/ ouwr;w;jci;u ouaocvurw ouwr;rueq;r (1) v|u|wi av|muxm;&rn/ Key Pair ouwr; (2) Epjynjy;ygu Key Pair topwppo;í ouaoc vurwtopjy|vy&e MOSS CA x av|muxm;Eiygon/

4.6.1 ouaocvurw ouwr;w;jci;tajctae

(Circumstances for Certificate Renewal)

ouaocvurwouwr;rueq;r xouaocvurwto;jy[ci;u quvuaqmi&u Ei&etwu im;&r;o;por ouaocvurwu ouwr;w;jci; (Renewal) jy[vy&e vtyyg on/

4.6.2 ouaocvurw ouwr;w;av[muxm;ci&o (Who Can Request Renewal?)

ouaocvurwav[muxm;ou,wi (o) tztpn;jzpygu tztpn;\ouaoc vurw av[muxm;jci;uprsm;aqmi&u&etwu w&m;0ipmjziwm0eay;tyxm;on u,pm; v,romv[i ouaocvurwouwr;w;jy[vy&e awmi;qEiygon/

4.6.3 ouaocvurw ouwr;w;jci;aqmi&ur

(Processing Certificate Renewal Request)

ouaocvurwouwr;w;jy[vy&mwi rvav[muxm;co trewu,jzpalumi; aocmap&e MOSS CA (o) RA r jyeíppaq;ygon/ Class 1 ouaocvurwtwu Challenge Phrase (or[wtvm;w Phrase) wpcu to;jy[íaomvn;aumi;? Private Key yiqijci;u ouaojyíaomvn;aumi;? Renewal Request uvucygon/ im;&r;o;porsm;on ouaoc vurw av[muxm;p0u jznpucaom Information rsm;Eitw Challenge Phrase (or[w tvm;w pum;p) wpccu a&;cs,ay;y&rn/ im;&r;o;poon Certificate topwpc jyevnjy[vyontcg ¤i;\ Challenge Phrase tygt0i av[muxm;p0u jznoi;caomtcsu tvursm;ajymi;vrr&cv[i ouwr;w;ouaocvurwu xway;ygrn/ ouwr;w; ouaoc vurw av[muxm;vmontcgwi;wi rvouaocvurwav[muxm;p0u CMOSS CA (o) RA r ppaq;onen;vr;rsm;Ei þ CP wi owrwxm;aom ppaq;&rn tcsursm;Eitn av[muxm;o\ Identity ujyevnppaq; twnjy[rn jzpygon/

4.6.4 ouaocvurwtop xw,Eialumi; im;&r;o;poo[talumi;lum;jci;

(Notification of New Certificate Issuance to Subscriber)

ouaocvurwtop xw,Eialumi; im;&r;o;poo[talumi;lum;jci;u ty' (4.3.2) twi;aqmi&uygon/

4.6.5 ouwr;w;jy; ouaocvurwrsm;u xwjyealunmay;jci;

(Publication of the Renewal Certification by CA)

ouwr;w;topjyevnxway;vuaom ouaocvurwu MOSS CA \ trsm;jyno lun&Eiaomouaocvurw rwwr;wu Ei RootCA\ trl;om;ouaocvurw rwwr; wu (National Repository) wwi xwjyealunmxm;rn jzpygon/

4.7 Key Pair toputo;jy\íouaocvurwouwr;w;jci; (Certificate Re-Key)

Certificate Re-Key on Public Key topwpcu to;jy\í ouaocvurwtopwpc xway;jci;jzpygon/

4.7.1 Key Pair toputo;jy\íouaocvurwouwr;w;&e tajctaersm;

(Circumstances for Certificate Re-Key)

Certificate Re-Key on ouaocvurwwpc\ vu&to;jyaeaom Private Key vjc\ pwc\&ru oo,&aomtcg (o) vu&o;paeaom Key rsm;\ouwr; (2) Epjynaomtcgwi jy\vyEiygon/ xuo ouwr;w;jci;u ouaocvurw ouwr;rueq;r (1) v lu\wi av\muxm;&rn/

4.7.2 ouaocvurwtop jyevnjy\vy&eawmi;qci&orsm;

(Who May Request Certificate of a New Public Key)

ouaocvurw ouwr;w;jci;twu Class 2 Ei Class 3 ouaocvurwrsm;jzpygu im;&r;o;pou,wiromv\i (o) tzltpn;\ ouaocvurwtwu vtyxm;aom w&m;0i u,pm;v,romv\i ouaoc vurwtop jyevnjy\vy&e awmi;qEiygon/

4.7.3 Key topto;jy\í ouaocvurwouwr;w;&e awmi;qjci;u aqmi&ujci;

(Processing Certificate Re-Keying Requests)

Key topto;jy\í ouaocvurwouwr;w;&e av\muxm;oon rvouaoc vurw av\muxm;o u,wi (o) w&m;0iu,pm;v, trewu,jzpalumi; ppaq;jci;Ei Authentication jzp&etwu owrwxm;aomvtycsursm;Ei avsmnpm jyevnppaq;jci;wu MOSS CA (o) RA on vyx;vyen;rsm;twi; Challenge Phrase (o) tvm;w Phrase wpcu to;jy\íaomvn;aumi;? Private Key yiqiru ouaojyíaomvn;aumi; aocsmpm ppaq;yg on/ xoppaq;atmijrijy;aom av\muxm;orsm;tm; ouaocvurwrsm;xway;jy; im;&r;

o;porm;xo ouwr;w; ouaocvurwxw,Eiaumi; taumi;lum;pm ay;yrn jzpygon/

4.7.4 Key topto;jyí ouwr;w;xm;aom ouaocvurwu xw,Eiaumi; im;&r;o;poo taumi;lum;jci;

(Notification of New Certificate Issuance to Subscriber)

Key topto;jyí ouwr;w;xm;aom ouaocvurwtopu xw,Eiaumi; im;&r;o;poo taumi;lum;jci;u ty' (4.3.2) twi; aqmi&uygon/

4.7.5 Key topto;jyí ouwr;w;xm;aom ouaocvurwtm;xwjyeaunm ay;jci; (Publication of the Re-Keyed Certificate by the CA)

ouwr;w;topjyevnxway;vuaom ouaocvurwu MOSS CA \ trm;jyno lun&Eiaom Website Ei RootCA \ trs;om;ouaocvurwrwwr;wu (National Repository) wwi xwjyeaunmxm;rn jzpygon/

4.8 ouaocvurwjyjyiajymi;vjci; (Certificate Modification)

4.8.1 ouaocvurw jyjyiajymi;vr tajctaerm;

(Circumstances for Certificate Modification)

ouaocvurwjyjyiajymi;vjci; (Modification)on im;&r;o;po\ Public Key rví vu&ouaocvurwwpcwiyg0iaomtcutvurm;ajymi;vraumi ouaocvurwtop wpc xway;&etwu avmuxm;jci;u &nne;ygon/ ouaocvurwjyjyiajymi;vjci; (Modification) on ty' (4.1) wiazmjyxm;aom ouaocvurwavmuxm;jci;Eiwnon[p0;pm;ygon/

4.8.2 ouaocvurwjyjyiajymi;v&eawmi;qci&o

(Who May Request Certificate Modification)

ty' (4.1.1) twi;aqmi&uygon/

4.8.3 ouaocvurwjyjyiajymi;vay;&eawmi;qrrsm;uaqmi&ujci;

(Processing Certificate Modification Requests)

MOSS CA **(o)** RA **on ouaocvurwjyjyiajymi;v&e avmuxm;o\ vtyaom tcsutvursm;tm; pprerppaq;jci;** (Identification **Ei** Authentication) **u ty' (3.2) twi; jyvyygrn/**

4.8.4 ouaocvurw topxwjy;alumi; im;&r;o;porsm;otalumi;lum;jci;

(Notification of New Certificate Issuance to Subscriber)

MOSS CA **(o)** RA **on ouaocvurwtopxwjy;ygu avmuxm;oxo t;ar;(v) (o) pm (o) tjcm;aomen;vr;rsm;u to;jyí talumi;lum;rn jzpygon/**

4.8.5 jyjyiajymi;vjy;aom ouaocvurwuvucjci;

(Conduct Constituting Acceptance of Modified Certificate)

ty' (4.4.1) twi;aqmi&uygon/

4.8.6 jyjyiajymi;vjy;aom ouaocvurwuxwjyeay;jci;

(Publication of the Modified Certificate by the CA)

ty' (4.4.2) twi;aqmi&uygon/

4.9 ouaocvurwy,zsujci;Ei,m,qi;ijci;

(Certificate Revocation and Suspension)

4.9.1 ouaocvurwy,zsujci;Ei,m,qi;i&etwu tajctaersm;

(Circumstances for Revocation and Suspension)

MOSS CA **(o)** Subscriber **u,wir y,zsu&e awmi;qrom ouaocvurwu y,zsuí** CRL **wi xwjyealunmay;ygon/ im;&r;o;pory,zsujci;jyvyvyguw&m;0ipmjzi a&;om;avmuxm;&rn/ ouaocvurwuy,zsu&etwu vavmuaomtaxmutxm;? talumi;jycsu&ygu** MOSS CA **on ,i;ouaocvurwu y,zsuEiygon/ atmuygtajc taersm; jzpay:cvi** CA **on im;&r;o;porsm;\ ouaocvurwrsm;u y,zsuEiygon/**

(1) MOSS CA **(o) im;&r;o;por ,i;** Private Key **c;,cc&vi (o) aysmuq;con [,lunvi (o) oo,&cvi ?**

(2) im;&r;o;poon vuem&rnpn;ur;rsm; (Subscriber's Obligation, Representation) (o) Subscriber Agreement yg tmrccsu (Warrenty) rsm;u cs;azmuon[MOSS CA r ,lunly; talumi;jycsursm;? ouaorsm;&cv\i ?

(3) im;&r;o;poEi csyqxm;aom oabmwncsupmcsyrsm; &yp/jy;q;om;v\i ?

(4) Class 3 Organization Certificate rsm;twu tz\tpn; (Affiliation) zsuor;v\i (o) r&awmv\i ?

(5) MOSS CA r ouaocvurwon Subject Field wi yg0ion trnr[wo wp0;tm; xway;xm;jci;? ¤i;y*\v\cijycsur&&y ouaocvurwu xway; on[,q\y; talumi;jycsu&cv\i ?

(6) ouaocvurwav\muxm;&mwi jznoi;xm;ontcsursm; rm;,i;aev\i ?

(7) ouaocvurwxway;jci;rjy\r y;wwijy&rntcsursm; jynpatmiaqmi&u jci; r&cv\i ?

(8) im;&r;o;po ? tz\tpn;trn ? ouaocvurwwiyg0iaom Common Name (CN) ajymi;vcv\i ?

(9) ouaocvurwygtcsutvursm;reuerr&alumi;Eiajymi;vom;alumi; ppaq; azmxwaw&cv\i ?

(10) ouaocvurwu quvuo;pygu Root CA ? MOSS CA Ei tjcm;o;porsm; tm; jyómjzpEicv\i ?

(11) ouaocvurwu w&m;r0ixw,xm;alumi;aw&&v\i ?

ouaocvurw quvu o;pralumi jyómjzpjci;& ? r& q;jzw&mwi atmuyg tcsursm;u xnoi;p0;pm;ygon/

(1) wiwe;r (Complaint) ta&twuEi oabmobm0 ?

(2) wiwe;rjy\vyoon rnorn0gjzponu xnoi;p0;pm;jci; ?

(3) vu&jyXme;xm;aom ouqion0ya'rsm; ? vyx;vyen;rsm;Ei uunr & ? r& ?

(4) im;&r;o;por ab;tE&m,jzpatmi to;jy\rrsm;alumi jzpay:vmaom wjyerrsm;?

ouaocvurwo;po\ Private Key c;,c&jci; ? aysmuq;jci; ? cs;azmuc&jci; (Compromise) jzpon[,qygu (o) o&ygu ouaocvurwo;poon MOSS CA o tjreq; quo,talumi;lum;&rn/

4.9.2 ouaocvurwy,zsu&eawmi;qci&o (Who can Request Revocation)

im;&r;o;pou,wi (Individual) (o) tz\tpn; ouaocvurwjzpygu wm0eay;ty xm;aom w&m;0iu,pm;v,rom y,zsu&eawmi;qEion/ im;&r;o;po\av\muvmu

Approve vyo MOSS CA Ei RA u,wirvn; ouaocvurwu y,zuEion (o) y,zu&e awmi;qEion/

4.9.3 ouaocvurwy,zu&e awmi;qrvyen;

(Procedure for Revocation Request)

ouaocvurwy,zu&e twuo;porm;r MOSS CA (o) RA o 'p*spw,vurw a&;x;xm;aom e-mail jziaomvn;aumi;? vu,wivma&muíaomvn;aumi; quo, talumi;lum;&rn/ ouaocvurwy,zujci;avmuvmypu MOSS CA \ URL jzpaom http://www.moss.com.mm wi Download &,Eiygon/

4.9.4 ouaocvurwy,zu&e qi;icse (Revocation Request Grace Period)

ouaocvurwu y,zu&e awmi;qrrm;twu qi;icserxm;yg/

4.9.5 ouaocvurwy,zu&eawmi;qjci;twu CA raqmi&u&elumjricse

(Time within which CA must process the Revocation Request)

MOSS CA on Revocation Request u ouqi&mwm0ec\ cijycsu&vi aEmiaE; luelumr r&apy (24) em&twi; owrwxm;aom tqirm;twi; vyaqmiom;ygrn/

4.9.6 Relying Parties r ouaocvurwy,zujci;u ppaq;&evtycsurm;

(Revocation Checking Requirements for Relying Parties)

Relying Parties rm;on rrto;jyrn ouaoc vurwrm;\ pwcs&rtajctae (Status) u ppaq;&rn/ ouaocvurw\pwcs&rtajctae (Certificate Status) u ppaq;&mwi -

1/ MOSS CA raemuq;xwjyecaom CRL (Most Recent CRL) u to;jyí ppaq;jci;?

2/ MOSS CA \ Web-Based Repository (o) OCSP (&ygu) ¤i;u to;jyí ppaq;jci;?

3/ Root CA raemuq;xwjyecaom CRL u to;jyí ppaq;jci; wjzivn; ppaq;Eiygon/

Relying Parties rm;on MOSS CA \ Repository Ei CRL rm;? National Repository? OCSP Responder (&ygu) rm;uto;jyí ouaocvurw\ pwcs&rtajctae (Status) u ppaq;Eiygon/

4.9.7 CRL xwjyeay;r tlurta&twu (CRL Issuance Frequency)

MOSS CA on ouaocvurwy,zupm&i;rm; ajymi;vrr&caom wpywwpurxw jyeay;rn/ CRL x& ouaocvurwwpc ouwr;ueq;jci; (Expire) jzpv|i ¤i; ouaocvurwu CRL r xwy,ay;rnjzpygon/ MOSS CA on im;&r;o;porm; \ ouaocvurwy,zupm&i;u y,zujy;on tcgwi;xwjyeay;rn/

4.9.8 ouaocvurwuy,zujci; trm;q;lumjrice

(Maximum Latency for CRLs)

MOSS CA r ouaocvurwwpcu y,zuontcg y,zujy;v|jy;csi; 4i;\ Repository wixwjyeay;rn/

4.9.9 ouaocvurwy,zuxm;jci; &?r& u On-line ppaq;jci;

(On-line Revocation/ Status Checking Availability)

CRL rm; Eiouaocvurwpwc&r tajctae (Certificate Status) rm; ppaq;jci;u Web-Based Repository Ei OCSP Responder (&&Eiv|i) o;í ppaq;Eiygon/ Web Address rm www. moss.com.mm jzpygon/

4.9.10 y,zuxm;aomouaocvurw[w/r[w On-line ppaq;jci; jy|vy&e v tycsurm;

(On-line Revocation Checking Requirements)

ouaocvurwu ,lunpwcsívucto;jyrno (Relying Party) rm;on rrto; jyrn ouaocvurw\ ,lunpwc&rtajctae (Status) u ppaq;&rn/ Relying Party on ouaocvurw\ ,lunpwc&rtajctaeu aemuq;xwjyecon ouqion ARL/ CRL uto;jyípaq;jci; rjyvyygu MOSS CA \ Repository Ei National Repository & ouaoc vurwtajctae (o) to;jyEion OCSP Responder (&yu) wu to;jyípaq;&rn/

4.9.11 Key c|;azmuc&jci;Eiouqiaom tx;aqmi&ucsurm;

(Special Requirements Regarding Key Compromise)

MOSS CA on rr\ Private Key c|;azmuc& (Compromise) on[aw&v|i (o) xojzpon[talumi;jycsuouaocivr&v|i ¤i;\ Potential Relying Party rm;tm; talumi;lum;jci;u wwEiorjyvyay;rn/

4.9.12 ouaocvurwu,m,qi;i&etajctaerm; (Circumstances for Suspension)

jyXme;xm;jci;r&yg/

4.9.13 ouaocvurwu,m,qi;i&eawmi;qci&orm;

(Who can Request Suspension)

jyXme;xm;jci;r&yg/

4.9.14 ouaocvurwu,m,qi;i&eawmi;qjci;vyie;pOrm;

(Procedure for Suspension Request)

jyXme;xm;jci;r&yg/

4.9.15 ouaocvurwu,m,qi;i&eowrwxm;aomumv

(Limits on Suspension Period)

jyXme;xm;jci;r&yg/

4.10 ouaocvurwpwc&rtajctae0eaqmirrm; (Certificate Status Services)

4.10.1 ouaocvurw\ vyie;aqmi&urtajctae (Operational Characteristics)

trm;Eiqiaomouaocvurw (Public Certificate) **rm;\ tajctaeu** CRL **rm;to;jy\í** Root CA **Ei** MOSS CA **** CPS **wiazmjyxm;aom** URL **&** Website ? LDAP Directory **Ei** OCSP Responder (**&yg u**) **wwi0ia&mu\un&Eiygon/**

4.10.2 ouaocvurwEiqiaom0eaqmir&&Eir (Service Availability)

ouaocvurwpwc&rtajctaeuppaq;\un&Eion0eaqmirrm; (Certificate Status Service) **u (24) em& (7) &u ywv; &&Ei&e aqmi&uxm;ygon/**

4.11 ouaocvurwim;&r; o;pjci;u tq;owjci; (End of Subscription)

ouaocvurw im;&r;o;poon atmuygen;vr;rm;jzi im;&r;o;pjci;u tq;ow Eion/

1/ rr\ ouaocvurwu topjyevnjy\vyjci; (Renewal) **or[w ouwr;w;jci;** (Re-Key) **wrjy\vyy ouwr;ueq;cijyjci; ?**

2/ ouwr;rueq;r rr\ ouaocvurwu y,z\uly; ouaocvurw topwpc tpm;rx;jci; ?

4.12 Private Key u Escrow vyjci;Ei jyevn&,jci; (Key Escrow and Recovery) jyXme;xm;jci;r&yg/

5. taxmutyrsm;? prcecjci;Ei vyie;aqmi&ujci;qi&m xe;csyrrsm; (Facility, Management and Operational Control)

5.1 MOSS CA vyie;\ &yyi;qi&mxe;csy? prxm;&rrsm; (Physical Controls)

5.1.1 pce;wnae&mEi aqmuvyjci; (Site Location and Construction)

MOSS CA **on 4i;\ vyie;rsm;u vyuiaqmi&u&mwi vlclr&ap&e ? rouqiorsm;r us;ausm0ia&mujci; ? to;jyjci;r&ap&e ? vW0uowi;tcsutvursm;Ei peprsm;u rouqio rsm;r lun&jci;rjylvyEi&e &yyi;qi&mumu,onyw0e;usi** (Physically Protected Environment) **u xm;&to;jyíaqmi&uygon/** MOSS CA **on vjclr&ap&etwu tce;rsm; wnaqmujci;u tvuxa&mepquo,aqmi&ua&;0ya' ? ,i;Eiqupyon en;0ya'rsm; ? trealumjimpmrsm; ? vr;necsursm;twi;aqmi&uxm;ygon/**

5.1.2 vyie;aqmi&u&mae&mo 0ia&mujci; (Physical Access)

MOSS CA **on 4i;\ pepvlcla&;twu tqi** (Tier) **rsm; cjcm;ly; vlcla&;ppaq;xm; ygon/ twi;yi;& vjclrtqiyjrionae&m** (Higher Tier) **rsm;u 0ia&muto;jy&e tjyiyi;& vjclrtqiyeronae&m** (Lower Tier) **rsm;u jzwausmly;r 0ia&mu&ygon/**

Tier **wi;u0ia&mu&e 0exr;u'rsm; ppaq;ly;rom 0ia&muEiygon/ xtce;rsm;o 0ia&mujci; ? to;jyjci;rsm;u** Digital Video Recorder **jzivn;aumi; ? vjcla&;rwwr;** (Log-File) **a&;oi;jci;jzivn;aumi; rwwr;wixm;ygon/ vjclon{&,m** (Secured Area) **tjzpowrwxm; aom ae&mrsm;o wu&uwm0e&orví tjcm;orsm;tm; 0ia&mucirjylyg/**

Cryptographic Material **rsm; xway;** (Create) **on ? or;qn;** (Store) **xm;on ae&mrsm;o 0ia&mujci; ? ppreaumi;taxmutxm;pppjci;** (Authentication) **u** Biometrics **en;ynmo;í** (2 Factor Authentication) **jzi xe;csyxm;ygon/** Server **rsm;? pm&upmwr;rsm;u aomcwxm;aom r;caowmrsm;** (Locked Safes) **? b'** (Cabinet) **rsm; ? ouqi&m** Container **rsm;xm;&í or;qn; xm;oygon/**

tx;wm0ejzi0ia&mu&e vtyony*lvrsm; 0i ? xujci;upu lu;luyrtz\ to trwjzi MOSS CA **wm0ecr cijylay;ygon/**

Sensitive CA Operation **rsm;jzpon** Certification Life-Cycle Process **rsm;u wi;luyon vlcla&;tptrrsm; xm;&aqmi&uygon/** (Certification Life-Cycle Process **rsm;rm ouaoc**

vurw xway;jci;rsm; (Issuance) ? or;qn;jci; (Storage) ? Key Ei ouaocvurwwqi&m ouwr;w;jci; (Renewal/Rekey) ? qi;ijci; (Suspension) ? y,zujci; (Revocation)w jzpygon/

5.1.3 r;tm;ay;pepEi avat;puxm;&aqmi&ur (Power and Air Conditioning)

- CA pep (System) quwutvyvyEi&e (Continuous and Uninterrupted Access) twu vlypp"gwtm;jywawmuom;jci;r&ap&e r;tm;ay;pepwi Online UPS Ei t&er;pursm; xm;&aqmi&uxm;ygon/
- tce;tycte? av0iavxu? avat;ay;pep? pxi;r (Humidity) wu Control jylvyxm; ly; ,i; System wivn; Primary Ei Backup peprsm;jzi cjcm;pp0aqmi&uxm;&ygon/

5.1.4 a&alumiysup;q;&;r (Water Exposures)

a&alumiysup;q;&;r r&ap&e vtyonpp0aqmi&urrsm; jylvyxm;ygon/

5.1.5 r;ab;tE&m,rumu,jci; (Fire Prevention and Protection)

r;ab;tE&m,r umu,Ei&e vtyonu&,mrsm;wyqijci;Ei umu,jir;owrn tptp0rsm; a&;qpraqmi&uxm;ygon/

5.1.6 Media rsm;xe;or;xm;&r (Media Storage)

Software rsm;? Data rsm;? Backup Information rsm; ? pm&i;pp Log File rsm; ? rwwr; File rsm;u tci&orsm;om lun&ei&e pepwuswm;q;umu,on peprsm;u pp0aqmi&uxm;yg on/ a& ? r; ? tjcm;aomobm0ab;tE&m,rsm;Ei ? ovu"gwrsm;alumi pm&upmwr;rsm; ? CD rsm; ? peprsm; ysup;q;&;r r&ap&e umu,xm;&ygon/

5.1.7 rvonpeypypn;rsm;zsup;peypr (Waste Disposal)

MOSS CA on to;rvonpeypypn;rsm;u pepwuspeyponen;vr;rsm; pp0 aqmi&uxm;ygon/ ta&;u;onowi;tcsursm;yg&onpm&upmwr;rsm; ? CD rsm; ? ypn; u&,mrsm;u peypjci;rjyr aocsmpmzsuq;ly;rom peyp&epp0xm;ygon/ ta&;lu;aom owi;tcsutvu (Sensitive Information) rsm;yg&on Media rsm; ? pm&upmwr;rsm;u zw&ír&Ei&e zsuly;rom peypygon/

5.1.8 vlcpwc&on tjcm;wpae&mwi Backup jy\vyor;qn;jci; (Off-Site Backup)

MOSS CA on Audit Log Data rsm;Ei ta&;lu;onowi;tcsutvu (Sensitive Information) rsm; yg0ion pep Data rsm;u vlcpwc&on tjcm;wpae&mwi Backup jy\vyí ae&mcjcm;ly; or;qn;xm;ygon/

5.2 vyie;qi&m xe;csyrrsm; (Procedural Controls)

5.2.1 ,lunpwc&orsm;u@ (Trusted Roles)

MOSS CA on ,lunpwc&onae&m (Trusted Position) wiwm0exr;aqmirn ,lun pwc&aomy*\vrsm; (Trusted Person) [owrw&mwiatmuazmjyyg vyie;rsm;uaqmi&u aeon 0exr;rsm;tm;v;? pmcsyEivyie;vyuio (Contractor) rsm;Ei tluay;? twiyicy*\v (Consultant) rsm; ? tvuxa&mepquo ,aqmi&ua&;A[tzEi lu;luyrtzr trepmjzi w&m;0i wm0eay;tyjci;c&orsm;tm;v; tus;0iygon/

Trusted Person rsm;wi MOSS CA \ Certificate Life-Cycle vyie;rsm;uaqmi&uorsm;? pepvjcla&;u wm0e,aqmi&uorsm; ? pep Authentication u Control vyci&orsm;Ei atmu azmjyygvyie;wu vyuiaqmi&uaeorsm; yg0iygon/

- Certificate Application wijznoi;xm;on tcsutvursm;u ppaq;o ?
- ouaocvurwtopav\muxm;jci; ? ouwr;w;av\muxm;jci; ? y,zsu&eav\mu xm;jci; (o) Enrollment Information rsm;u vucjci;? jii;y,jci;rsm;uaqmi&uorsm;?
- ouaocvurwrsm;u xway;jci; ? qi;ijci; ? y,zsujci;aqmi&uorsm;? ouaoc vurw rwwr;rsm; (Repository/ LDAP /OCSP (&ygu) \ ueowxm;aom ae&mrsm;o 0ia&mujy\yiajymi;vjci; ? xnoi;jci; ? zsujci; aqmi&u&e tci&otm;v;) ?
- im;&r;o;porsm;Ei ywouaom tcsutvursm; ? Request rsm;u uiw,ajz&i;orsm;?
- Customer Service uaqmi&uaom0exr;rsm; ?
- Cryptographic Service uaqmi&uaom 0exr;rsm; ?
- vjcla&; 0exr;rsm; ?
- System Administrator rsm; ?
- ouqiontii*sie,mrsm; ?
- Infrastructure \vlcpwc&r twu praqmi&uo txutqit&m&rsm; yg0iygon/

MOSS CA r ,lunpwc&aomy*\v (Trusted Person) rsm;on owrwxm;aom t&ntcsi;rsm; ? owrwcsursm; (Screening Requirement) Ei jynpuunr&ygon/

5.2.2 vyie;wpcc:i;ptwuv tyrn0exr;ta&twu

(Number of Persons Required Per Task)

MOSS CA onwi;u:yaomvyx;vyen; (Control Procedure) rsm; owrwxm;&ly; xtwi;aqmi&ur&ap&e wm0e (Duty) rsm; o;jcm;ca0c:xm;jci; ? ta&;u;on vyie;rsm;wi 0exr;rsm; wp0;xuru wm0e,aqmi&urom jy;ajrmu&eca0aqmi&uapjci;jzi xe;cdyr (Control) jy{vyxm;ygon/

tvy0w&m;tvu wm0e,aqmi&ur aoc:map&etwu vyx;vyen; (Policy) rsm; ? Control Procedure rsm; xm;&ygon/ ta&;u;on Cryptographic qi&m Hardware rsm; ? HSM rsm; ? Signing Unit rsm; ? ouqion Key Material rsm;u vwp0;xuruxm;&vyaqmirom jy;ajrmu aprn jzpygon/

Internal Control Procedure rsm;taejzi vlcrtwuta&;u;on tc:utvursm;? puypn;u&,mrsm;u uiw,aqmi&u&mwi (Physical Access or Logical Access tygt0i) ten;q;v (2) a,muxm;&ly; aqmi&urom vyie;ly;ajrmuatmi aqmi&uEirn tptp0rsm; xm;&aqmi&uygon/ ypn;rsm;uuiw,to;jy{í vyie;aqmi&u&mwi wp0;wn;Ei vyie; tprtq;o aqmi&uEijci; r&ap&e Control rsm;u ca0xm;ygon/

ouaocvurw av{muvmwpapmia&muvmonrpí ppaq;jci; ? ouaocvurw xway;jci; ? ouwr;w;jci; ? y,z:ujci; ? aemuq;wiz:uq;ypjci;pon Life-Cycle wpcv; u ,lunpwc:&on 0exr;rsm;xm;&ly;aqmi&uygon/ Physical Access Ei Logical Access u ta&;u;onae&mrsm;wi o;jcm;vrsm;uo;í cjcm;xm;ygon/

5.2.3 0exr;wp0;c:i;p\vyie;wm0ersm;Eippaq;ru@

(Identificationand Authentication for each Role)

MOSS CA \ ,lunpwc:&aom0exr;tjzpcexm;rn vjcla&;tqijrit&m&rsm; (Top Level Security Related) tm;v;uvawppaq;jci; ? rwywiEi tjcm;vtyaom taxmutxm;rsm; to;jy{í ppaq;jci;rsm;aocmpmjy{vyly;rom 0exr;tjzpcexm;ygon/ vtyygu Background Check rsm; jy{vyly;r cexm;ygon/ 0exr;tjzp cexm;ly;aemu ouqi&m txuv{u; \ oabmwnc:ujziom pm&upmwr;rsm; ? ueyewmEi qupyypn;rsm; ? Software rsm;u uiw,o;p (Access) ciay;jci; ? tvuxa&mep Data rsm;u lun&ci ? vyie;vyaqmici ay;jci;w jy{vyygon/

5.2.4 vyie;wm0ersm;ca0r (Roles Requiring Separation of Duties)

vyie;wm0ersm; ca0owrwjci;wi atmuygwyg0iygon/

- ouaocvurwav\muxm;jci;wi yg0iaom tcsutvursm;u ppaq;jci;?
- ouaocvurwav\muxm;jci;?y,zsujci;?ouwr;w;jy\vyjci;?tcsutvursm;pm&i;a&;oi;jci;wu vyaqmijci;?
- ouaocvurwjy\vyjci;?xway;jci;?ouwr;w;jy\vyjci;?y,zsujci;?zsuq;jci;Ei ouaocvurwrwwr;wu (Repository) wi Publish jy\vyjci;?
- im;&r;o;po\ tcsutvursm;?awmi;qjci;rsm;u uiw,ajz&i;jci;?

5.3 0exr;yi;qi&mxe;cstyrrsm; (Personnel Controls)

5.3.1 0exr;rsm;\ t&ntcsi; vyie;tawtlu\ Ei Clearance vtycsursm;

(Qualifications, Experience, and Clearance Requirements)

,lunpwcs&aom 0exr;tjzp av\muxm;orsm;on ¤i;w\ aemualumi;&mZ0i (Background) ?ynmt&ntcsi;?rrwm0e,aqmi&urn vyie;Eiywouaom vyie;tawtlulwu jynppm wijyav\muxm;&rn/ vtyygu ,civyie;rsm;r &i;vi;r (Clearance) u,&rn/ Trusted Position wi&aeon 0exr;rsm;tm; aemualumi;&mZ0i ppaq;jci; (Background Check) u ten;q;(5) Epwp\urjyevnjy\vyygon/

5.3.2 0exr;\aemualumi;&mZ0ippaq;jci;jy\vyonvyie;p0rsm;

(Background Check Procedures)

jyXme;xm;jci;r&yg/

5.3.3 0exr;rsm;twuoiwe;ycsrrsm; (Training Requirements)

MOSS CA \ 0exr;rsm;u vtyaomoiwe;rsm; tcgtm;avsmpm pp0ycsay;ygon/ oiwe;ay;&mwi wp0;csi;p\ vyie;wm0etvu atmuygwu oilum;ygon/

- Basic PKI Concept
- Job Responsibilities
- Security (Physical, Network, System) and Operational Policies and Procedures
- Use and Operation of Deployed Hardware and Software
- Incident and Compromise Reporting and Handling
- Disaster Recovery and Business Continuity Procedures

5.3.4 oiwe;jyevnycsjci;tlurta&twuEivtycsursm;

(Retraining Frequency and Requirements)

vtyov jyXme;ygon/

5.3.5 vyie;wm0eca0csxm;jci;Eivnvnajymi;vcsxm;jci; tptp0

(Job Rotation Frequency and Sequence)

vtyov jyXme;ygon/

5.3.6 tcir&baqmi&urrsm;uywyiwm;jrpjci; (Sanctions for Unauthorized Actions)

MOSS CA **Ei ,i;** RA **rsm;\ 0exr;rsm;r tcir&baqmi&urrsm; (o)** MOSS CA **Ei** RA **0exr;rsm;r ay:vpEi vyx;vyen;rsm; azmuzsurrsm;u lu;luyrtzowijyjy; ta&;, aqmi&uygon/ us;veon tlura&Ei azmuzsurtwi;twmay:rwní xuoiaom jyp'Pay;jci;? tvyrxwy,jci;Eiw&m;0ya't& ta&;,jci;wtx aqmi&uygon/**

5.3.7 vyie;ciwm0exr;aqmi&evtyaom pm&u?pmwr;rsm;

(Documentation Supplied to Personnel)

ouqi&m0exr;rsm;tm; vyie;ciwm0eausyepmxr;aqmi&evtyaom oiwe;rsm;? vr;nersm;?pm&u?pmwr;rsm;u ay;xm;ygon/

5.4 pm&i;pp rwwr;jylvyjci;tptrrsm; (Audit Logging Procedures)

5.4.1 rwwr;or;qn;xm;&rntjzptysursm; (Types of Events Recorded)

MOSS CA **on** Manual Log **(o)** Automatic Log **rsm;xm;&ly; atmuazmjyyg tjzptysursm; twu pm&i;pprwwr;xm;&ygon/ rwwr;xm;&aomtjzptysuwi;wi ae&u? tcseEi þtjzptysuu jzpay:apon talumi;&i;wyg0iygon/**

1.vyie;aqmi&ujci;qi&m tjzptysursm;-

- CA Key **rsm;jylvyjci;**?
- CA **pepEi** Application **rsm;** Start-Up **Ei** Shutdown **jylvyjci;**?
- CA **\taO;pwtcsutvursm;Ei** Key **ajymi;vrrsm;**?
- Cryptographic Device **rsm;** Life-Cycle Management **qi&m tjzptysursm;**?
- CA Private Key **Eiqiaomvyie;twu** Activation Data **rsm;yiqirEi vyie; aqmi&uonae&mrsm;o 0ia&mujci;rsm;**?

- System Configuration ajymi;vrrsm;Ei Maintenance aqmi&urrsm; ?
- im;&r;o;porsm;\ tcsutvursm; ? Activation Data ? Key Eiywouon tcsutvursm; yg0iaom Media rsm;u zsuq;jci;rwwr;rsm; ?

2. ouaocvurw im;&r;o;porsm;\ Life-Cycle Management qi&m tjzptysursm;
   - ouaocvurwavlmuxm;jci; ? ouwr;w;jci; (Re-Key/Renew) ? y,zsujci; rsm; ?
   - ouaocvurwrsm; ? CRL rsm; ? Generate jylvyjci; ? Issue vyjci;qi&m rwwr;rsm; ?
3. ,lunpwcs&aom0exr;rsm;\vyie;aqmi&urrsm;-
   - Logon discrepancy and Logoff lu[;pm;rrsm; ?
   - Privileged User rsm;\ System Privileged ajymi;vrrsm; ? Password xm;&jci;rsm; ?
4. uunrr&jci;Ei cs;azmujci;rsm;-
   - CA pepEi ue,utwi;ol cijylcsur&b 0ia&mu&elu[;yr;rrsm; ?
   - vl0uzirsm; ? rwwr;rsm; zwjci; (Read Access) ? a&;jci; (Write Access) ? zsuq;jci;rsm; (Deletion) ?
5. ouaocvurwEi ouaocvurwrwwr;wu (Repository) ay:wi zwjci; ? a&;jci; w aqmi&ur&&rrsm; ?
6. ouaocvurwjylvyjci;qi&mr0g'ajymi;vrrsm; (0yrm-Validity Period ajymi;vjci;)
7. taxax
   - vjcla&;qi&mrwwr;rsm;Eixrwwr;rsm;(SecurityProfile)wiajymi;vjylyixm;rrsm;?
   - pep,m,cs[,i;;jci; (Crash) rsm;? Hardware Failures rsm;Ei tjcm;aom yrer[w on up&y (Anomalies) rsm; ?
   - Firewall Ei Router Activity rsm; ?
   - MOSS CA vyie;ciwi Tier tvu{n0i ?{nxu&rrsm; ?

Log ziwi a&;om;rwwr;xm;on tcsutvursm;rm atmuygtwi;jzpygon/

- trwp0 Automatic Journal Entry rsm;twu Sequence Number ?
- 0i?xuonae&u ? tcse Ei talumi;t&m ?
- rwwr;pmtywi a&;oi;&ygu rwwr;wio\trn ?

8.A[tz?lu;luyrtzEi Root CA wr rwwr;tjzp or;qn;&e vtyon[nelum; xm;aom tcsutvursm;/

5.4.2 rwwr;rsm;u praqmi&ujci;lurEe; (Frequency of Processing Log)

Audit log file rsm;u ppaq;&mwi Audit log file rsm;u jyevno;oyjci;Ei ta&;ygaom tjzptysursm;u Audit log summary wi a&;om;rwwr;xm;jci;rsm; yg0iygon/ Audit Log File rsm;u jyevno;oyjci; jylvy&mwi log rwwr;rsm;wi jyljyixm;rrsm; &?r& ppaq;jci;Ei Audit log a&;om;csursm;tm;v;u jyevnppaq;jci;?yrer[waom uprsm;?oway;csursm; (alerts) u ppr; ppaq;jci;rsm; yg0iygon/

ta&;ygon vlcla&;qi&mtjzptysursm; ?up&yrsm;twu wpywvli ten;q; wplur ppaq;rrsm;jylvyygon/ ¤i;tjyi MOSS CA on ¤i;\ Audit Log File rsm;r oo, jzpEion or&;usr[waom ?yrer[waom tjzptysursm;u tlrwr; ppaq;ly; oway;csu xwjyejci; ?ppr;ppaq;jci;rsm;jylvyygon/ Audit log review jylvyxm;onrsm;uvn; rwwr;xm;&ygon/ MOSS CA \ vyie;qi&m rwwr;rsm;u Root CA o (6) vvliwplur wijyygon/

5.4.3 Audit rwwr;rsm;xe;or;xm;&jci; (Retention Period for Audit Log)

Audit rwwr;rsm;u rwwr;wijy;ten;q; (2) vlumontx vyie;vyaqmion ae&mwi xe;or;xm;&ly;aemuyi;wi vlcpwcs&onae&mü ty' (5.5) wi azmjyxm;on twi; rwwr;a[mi;tjzp or;qn;xm;&ygon/

5.4.4 Audit rwwr;rsm;uumu,jci; (Protection of Audit Log)

Audit rwwr;rsm;u rormorsm;r 0ilunjci;?jyiqijci;?zsuypjci; (o) tjcm;rorm onuprsm; rjylvyEi&e tvuxa&mepen;jzi umu,wm;q;onpeprsm; jylvyxm;ygon/

5.4.5 Audit rwwr;rsm; Backup aqmi&urntptp0 (Audit Log Backup Procedures)

Audit Log rsm;u aep0vyie;vyaqmior\ Backup jylvyly; wpywwplur tjynt0 (Full Backup) jylvyygon/

5.4.6 Audit rsm;ppn;r pep (Audit Collection System (Internal vs. External))

tvtavsmu Audit Data rsm;xwjci; ? rwwr;xm;jci;wu Application / Network Ei Operating System Level rsm;twi; aqmi&uygon/ MOSS CA Ei RA 0exr;rsm;r Manual Audit Data rsm;u rwwr;xm;&ygon/

5.4.7 jzpEiajc&aom xcuysup;rrsm;u wi;wmppaq;jci;

(Vulnerability Assessments)

jzpEiajc&aom xcuysup;rrsm;u atmuygae&mrsm;wi wi;wmppaq;rjyvy&rn/ pep wpcv;\ jzpEiac&aomysup;q;&;rrsm;wi;wmppaq;jci;u Log Data rsm;wi rwnppaq;y; aep0 ? vp0Ei Epp0 jyvyygon/

(u) CA pep\ Software/ Hardware yi;rsm; ?

(c) Physical Facilities rsm; ?

(*) Network peprsm; ?

(C) pm&i;ppjci;qi&m tjzptysursm; (Events in the Audit Process) ?

5.5 Record rsm;rwwr;a[mi;xm;&r (Records Archival)

5.5.1 rwwr;a[mi;xm;&&rn rwwr;trs;tpm;rsm; (Types of Records Archived)

MOSS CA on atmuazmjyygupr sm;twu rwwr;xm;&ygon/

- paqmi;&&on pm&i;pptcsutvu (Audit Data) tm;v; ?
- ouaocvurwxway;jci;Ei ouqion y;wygtaxmutxm; ? pm&upmwr; (Support Document) rsm;tm;v; ?
- Certificate Life-Cycle qi&mtcsutvutm;v; ?
- A[tz? lu;luyrtzEi Root CA \ nelum;csujzi rwwr;xm;&&rn tjcm; tcsursm; ?

5.5.2 rwwr;a[mi;xe;or;xm;&rnumv (Retention Period for Archive)

MOSS CA \ ouaocvurw xway;jci;qi&m rwwr;rsm;u ouaocvurw ouwr;uejci; (o) y,zsuonaerpí ten;q; atmuazmjyygaetx rwwr;or;qn;xm;& ygon/

- Class-1 ouaocvurwrsm;twu (5) Ep
- Class-2 Ei Class-3 ouaocvurwrsm;twu (10) Ep

5.5.3 rwwr;a[mi;rsm;u umu , xm;&r (Protection of Archive)

xor;qn;xm;on rwwr;a[mi;rsm;u tci&orsm;uom lun&cijy(í rouqi orsm;r lun&jci; ? jyiqijci; ? zuq;jci; ? rwwr;rsm;wi jy(yijci;rsm;rjy(vyEi&e umu , xm; &ygon/ þ CP wi azmjyxm;on owrwxm;on rwwr;rsm;\ ouwr;twi;ysup;rr& ap&e pepwus xe;or;xm;&ygon/

5.5.4 rwwr;a[mi;rsm; Backup xm;&rntptpO (Archive Backup Procedure)

ouaocvurwrsm;\ tcsutvursm;u aepO Incremental Backup ? tygwpO Full Backup jy(vyygon/

owi;tcsutvursm;u rwwr;a[mi;tjzp xm;&&mwi trsm;pu tvuxa&mep Record ypjzixm;&? vtyygu pm&upmwr;ypjzi or;qn;jy; xrwwr;rsm;u vjcon tjcm; wpae&mwi rwu;í xe;or;xm;&rnjzpjy; ysup;r(r&ap&evn; twwEiq; pepwuspO or;qn;xm;&ygon/

5.5.5 rwwr;rsm;\ tcserwom;jci;qi&m vtycsursm;

(Requirements for Time-Stamping of Records)

ouaocvurwrsm;? CRL rsm;? tjcm;aomy , zsujci;qi&m rwwr; (Revocation Database) rsm;wi tcseEi ae&uu rwom;xm;ygon/ CA Computer System \ Time Clock u ppr;ppaq;rrsm;wi u;um;to;jy(Ei&etwu a'opawmcseEi uunr&ap&e aqmi&uxm;& ygon/ xuo tcseqi&mrwom;rrsm;on Cryptographic ay:wi tajcc&ervyg/

5.5.6 rwwr;tcsutvursm;ppn;r (Archive Collection System (Internal or External))

MOSS CA \ rwwr;a[mi;paqmi;onpep (Archive Collection System) xm;&ygon/ MOSS CA \ ,lunpwcs&aom 0exr;rsm;rom rwwr;tcsutvursm;u vyuiaqmi&uci &ygon/

5.5.7 rwwr;rsm;&&r Ei ppaq;r vyie;pOrsm;

(Procedures to Obtain and Verify Archive Information)

tci&orsm;Ei ,lunpwcs&orsm;om rwwr;a[mi; (Archive Data) rsm;u 0ia&mu lun&ci&ygon/ rwwr;rsm;tm; jy(yiajymi;vom;jci; & ? r& (Integrity of the Information) u jyevnor;qn;on tcgwi; (Restore jy(vyon tcgwi;) jyevnppaq;ygon/

5.6 CA Key Pair topjyvyjci; (Key Changeover)

MOSS CA \ owrwxm;aom Key ouwr; (Maximum Life Time) u ausmveygu CA Key Pair rsm;uvyie;wi quvuto;rjyyg/ MOSS CA Key Pair ouwr;rueq;rten;q; (12) v lulwií ouwr;w;jci; jyvy&rn/ MOSS CA Key Pair topwppvtyontcgwi; xwygon/ (0yrm- CA KeyPair ta[mi;utpm;x;&e?vu& Key Pair \ jznzutjzp to; jy&e?0eaqmir toprsm;ay;&e)

CA Key Pair ta[mi;r topou;ajymi;&mwi v,uacsmarlpmu;ajymi;Ei&e Key ajymi;vjci; vyx;vyen;rsm; (Key Changeover Procedure) rsm;u lulwiowrwxm;ygon/

- Key ajymi;vjci;rjylvyr MOSS CA on im;&r;o;porsm;o ouaocvurw xway;jci;u ten;q; (12) v lulwií &yem;ygon/
- Certificate Key Pair &ypjy;aemuyi; ouaocvurwim;&r;o;porsm;u CA Key Pair topo;í Sign x;rnjzpygon/
- rv Key Pair ouwr;ueq;jci;rjzprtx CRL rsm;urv Key Pair o;í xwjyeygon/
- ouaocvurwta[mi;ouwr;rueq;r (12) v lulwií ouaocvurwtopu xwjy; Supplement tjzp to;jylygon/

5.7 CA tcsutvursm;wucuc&rEiab;tE&m,usa&murrsm;rjyevnxaxmijci;

(Compromise and Disaster Recovery)

5.7.1 rawmwqrEicsl;azmuc&rrsm;u uiw,ajz&i;rn vyx;vyen;rsm;

(Incident and Compromise Handling Procedures)

MOSS CA \ tcsutvursm;? (ouaocvurw avlmuxm;jci;qi&m tcsutvursm;? pm&i;pp Data rsm;? xway;xm;aom Certificate rsm;\ database records rsm;) \ Backup uvjcl on tjcm;wpae&mwi xe;or;xm;&ly; rawmwqrEi cs;azmuc&rrsm;jzpym;ygutqioi &&Ei&e aqmi&uxm;ygon/ MOSS CA on rawmwqrEicsl;azmuc&rrsm;u uiw,ajz&i;rn tptrrsm; aqmi&uxm;&ygon/ ,i;tptrwi ten;q;atmuazmjyygtcsursm; yg0iygon/

(1) CA Key cs;azmu?c;,c&jci;?ysuq;jci;?

(2) CA pepEi ue,utwi;o rormorsm;0ia&mujci;?tcsutvursm;jylyic&jci;? zsuq;jci;?c;,c&jci;?

(3) ouaocvurwuw&m;r0ixw,c&jci;?qi;ic&jci;?y,zsuc&jci;?

5.7.2 ueyslwmEi qupyypn;rsm;? aqm0vEi tcsutvursm; ysup;q;&;ru aqmi&ujci; (Computing Resources, Software and/ or Data are Corrupted)

ueyslwmEi qupyypn; (Computing Resources) rsm;? Software rsm;? Data rsm;pon wwi ysup;q;&;r (Corruption) rsm; jzpym;ygu lu;luyrtz Ei Root CA otp&icpmwijyly; MOSS CA \ vlcla&;Eirawmrqrrsm;u uiw,ajz&i;rn vyx;vyen;rsm; (Incident Handling Procedure) twi; aqmi&uygon/ xvyx;vyen;rsm;wi ueyslwmEi qupyypn; (Computing Resources) rsm;? Software rsm; ? Data rsm; ponwu oiavsmonae&moa&lajymi;jci; ? rawmwqruppr; ppaq;jci; (Incident Investigation) Ei jyevnajz&i;rn en;vr;rsm; yg0iygon/ vtyygu Key Compromise Ei Disaster Recovery Procedure rsm; a&;qjyXme;ygon/

5.7.3 Private Key cs;azmuc&jci; twu aqmi&urvyie;p0rsm;

(Entity Private Key Compromise Procedures)

MOSS CA \ Private Key (o) Infrastructure rsm; cs;azmuc&jci; (Compromise) jzpon[oo,jzpygu (o) o&ygu (o) xo jzpysuon[taxmutxm;civygu MOSS CA r tzlzly; tajctaeuavvmqe;ppjci; ? lu;luyrtzEi Root CA otp&icpmwijyjci; ? Action Plan a&;qjci; ? Action Plan twi; taumitxnazmjci;rsm;u tqiqivyaqmiom;rn jzpygon/ tu,í MOSS CA \ ouaocvurwuy,zsu&e vtyygu-

- xoy,zsualumi;u MOSS CA \ Repository Ei National Repository wi xnoi; alunmly; ouqiorsm;tm; wwEiors talumi;lum;ay;rn jzpygon/
- CA tjzpr&ypjci;uprví Key Pair topwpp xwjy; Root CA xr ouaoc vurwtopwpc&,rn jzpygon/

5.7.4 obm0ab;tE&m,usa&mujy;aemu vyie;rsm; quvuvnywEirpr;&n

(Business Continuity Capabilities After a Disaster)

MOSS CA on ab;tE&m,rsm;alumi ysup;q;&;r ? xcurrsm;jzpym;ontcg vyie; quvu aqmi&uEiap&e yirae&mra0;umon tjcm;wpae&mwi Disaster Recovery Site xm;& jy; v (o) obm0alumi tE&m,rsm;jzpym;ygu vyie;quvuvnywEi&etwu Recovery Plan u a&;qxm;ly; pr;oyjci;uvn; aqmi&uxm;ygon/ wuEiorysuq;q;&;r en;ap&e aqmi&uxm;ygon/ þ Plan u Disaster jzpym;ygu vyie;aqmi&uEiap&e yreppaq;jci; ? cseuujci; ? ajymi;vjyfjyijci;rsm; jylvyygon/ t"u CA vyie;rsm;jzpon -

- ouaocvurwxway;jci; ?

- ouaocvurwy,zujci;?
- ouaocvurwy,zujci;qi&mtcutvurm;xwjyejci;rm;utcewtwi;jyevn aqmi&uEi&eppOxm;&ygon/

MOSS CA \ Disaster Recovery Database uvn; yir Production Database Ei uunr &ap&e aqmi&uxm;&ygon/ ab;tE&m,jzpym;ly; wpywtwi; Full Recovery &&&etwu Disaster Recovery Plan a&;qxm;ygon/

MOSS CA on Disaster Recovery Facility twu puypn;rm;Ei Software rm;ut&e Ei Backup rm;xm;&ygon/ ab;tE&m,jzpygu jyevnxaxmiEi&e MOSS CA \ Private Key uvn; Encrypted ypjzi Backup xm;&ygon/

5.8 CA (o) RA tjzpr vyie;&ypjci; (CA (or) RA Termination)

MOSS CA r vyie;&ypygu im;&r;o;porm;? Relying Party rm;tm; xcuepemr ten;q;jzpaprn Termination Plan u a&;qxm;ygon/ Termination Plan wi atmuygtcurm; twi; praqmi&uygon/

- tjcm; CA rm;? im;&r;o;porm;Ei ouqiotm;v;tm; lulwitalumi;lum;jci; jylvy ygrn/ xtcerpí MOSS CA on rnon ouaocvurwxway;jci;ur rjylvyy?
- CA vyie;rm;&ypjci;jylvyawmrntalumi; Website Ei owi;pmrm;wivtrm;oom ap&e lulwixwjyealujimay;jci;?
- MOSS CA \rwwr;a[mi; (Archive) rm;? rwwr;rm;? Database rwwr;rm;Ei pm&upmwr;rm;u &yponaerpí þ CP wi owrwxm;onumvtx xe;or;xm;& jci;?
- MOSS CA \ Repository Ei CRL u &ypjy;onaerpí (12) vtx trm;jyno 0ia&mu lun&Eiatmi ppOxm;&jci;?
- Customer Support 0eaqmir (Service) rm;u quvu o;pEi&eppOjci;?
- CRL rm;xwjyejci;? ouaocvurw,lunpwc&rtajctaeppaq;on 0eaqmir (Certificate Status Checking Service) rm; quvuaqmi&uEi&e prjci;?
- ouwr;rueq;ao;aom ouaocvurwtm;v;u lulwitalumi;lum;umv jynajrmu on tcewiy,zujy;jzpatmi aqmi&ujci;?
- vtyygu Subscriber rm;u Refund ay;&e (o) tpm;x; ouaocvurwrm;xway;&e ppOaqmi&ujci;?

- CA \ Private Key Ei Hardware Token rm; Disposition jy vyjci; ?
- CA \ 0eaqmir (Services) rm;u qucrntjcm; CA ovajymi;ay;ty&eaqmi&ujci; ?
- vyie;v;0&yprn ae&uEi &yprn tptp0u Root CA owijyjci; Root CA r MOSS CA \ ouaocvurwuy,zujci;Ei vtyyguim;&r;o;porm;\ouaocvurwrm; uyg y,zujci; /

6. en;ynmqi&m vjcla&; xe;cyrrm; (Technical Security Controls)

6.1 Key Pair jy vyjci; Ei Installation jy vyjci; (Key-Pair Generation and Installation)

6.1.1 Key Pair jy vyjci; (Key-Pair Generation)

Key Pair Generate jy vy&mwi ,lunpwc&onpeputo;jyjci; ? Key rm;u owrw xm;aom Cryptographic t&ntao;twi;jy vyjci;Ei Private Key rm;u rouqiorm;r to; jyjci; ? jyjyiajymi;vjci; ? xwazmajymqjci; ? aymuq;jci; tp&onwr umu,jci;rm;u aqmi&uxm;ygon/ MOSS CA \ Key generate jy vyjci;u lu wia&;qxm;on Key Generation Ceremony twi; aqmi&uxm;ygon/

im;&r;o;porm;twu Key Pair tm;v;u lu wiowrwxm;on owrwcurm;twi; Generate jy vyygon/ Key Generate jy vyonvyie;p0u jyiy Network Ei Internet cwquxm; jci;r&aom o;oeowrwxm;on ueylwmwiomjy vyygon/ CA Key Pair Generation Eiou qionvyie; (Activities) tm;v;uae&u ? tceEiwu rwwr;xm;&y; yg0ivyaqmiotm;v; r vurwa&;x;ygon/ prtycyor owrwxm;onumvtx xrwwr;rm;u vtyov ppaq;jci; (Audit) ? jyevnlun&rrm; (Tracking) jy vyEi&e or;qn;xm;ygon/

6.1.2 ouaocvurw im;&r;o;porm;o Private Key ay;yjci;

(Private Key Delivery to Subscriber)

RA Ei Subscriber rm;\ Key Pair rm;u MOSS CA r Generate jy vyygu Handware Token (o) Device rm;u vjcpwc&aomen;o;í ay;yjzea0ygon/ Device u Activate jy vy&e vtyaom Data u RA (o) Subscriber o ay;yygon/ xoay;yjci;rm;uvn; rwwr;xm;& ygon/

MOSS CA r Key Pair xway;ygu Private Key uouaocvurwtr;tpm; (Class 2, Class 3) twu im;&r;o;pou,wi RA xo vma&muí xw,&e vtyygon/

6.1.3 CA \ Public Key u Relying Parties rsm;rto;jy|Ei&e ppOaqmi&uxm;jci;

(CA Public Key Delivery to Relying Parties)

MOSS CA \ ouaocvurwEi im;&r;o;porsm;\ ouaocvurwtm;v;u ,i; CA \ Website jzpaom www.moss.com.mm wi Download jy|vyEi&ewixm;ygon/ im;&r;o;porsm;\ ouaocvurw& Certificate Chain wi Root CA Ei MOSS CA \ ouaocvurwEitw Full Certificate Chain tm;v;yg0irnjzpygon/ S/MIME Protocol u to;jyaom Relying Party rsm;Ei ouaocvurwto;jyorsm;on 4i;w& MOSS CA ouaocvurw \ Validity u o&&e Certificate Hash Value u Website & Hash Value Ei wuqippaq;&rn/ MOSS CA ouaocvurwu Root CA \ National Repository jzpaom www.rootca.org.mm/repository wivn; azmjyxm;rnjzpygon/

vtyygu Root CA Ei MOSS CA \ ouaocvurwrsm;u Download jy|vyírr\ Computer wi Install jy|vyEiygon/

6.1.4 Key \t&,tpm; (Key-Sizes)

Key-Pair rsm;\ Private Key rsm;u Cryptanalysis jy|vyjci;en;jzi o&atmijy|vyjci;rumu,Ei&e vavmuaom Key t&n (Key Length) xm;&ygon/ MOSS CA \ Key Length rm (2048) Bit RSA jzpygon/ RA Ei im;&r;o;porsm;\ Key Pair Size on (1024) Bit jzpygon/ vurwa&;x;&etwu to;jyaom Hash Algorithm rm SHA1 jzpygon/

6.1.5 Public Key Parameter jy|vyjci;Ei t&ntao;ppaq;jci;

(Public Key Parameters Generation and Quality Checking)

ouqijci;r&y/

6.1.6 Key to;jy&on&n&,cu (Key Usage Purpose as per X.509 V3 Key Usage Field)

MOSS CA \ Key u atmuy&n&,cursm;jziom to;jyygon/

- im;&r;o;porsm;\ ouaocvurwu 'p*spw,vurwa&;x;xway;&e?
- CRL rsm;xway;&ewjzpygon/

6.2. Private Key umu,jci;Ei Cryptographic Module o;pxe;cyjci;rsm;

(Private Key Protection and Cryptographic Module Engineering Controls)

MOSS CA on Physical?Logical Ei Procedural Control rsm;ayi;pyum ,i;\ Private Key u trewu,vlcpwcr&ap&e praqmi&uxm;ygon/ ouaocvurwim;&r;o;porsm;tm;

rr\ Private Key jyiqic&jci; ? aysmuq;jci; ? owpyg;rto;jyjci; ? tjcm;orsm;tm;xwazm ajymlum;jci; (Disclosure) rsm;u umu,&evtyaom lulwiumu,rrsm;jylvy&e toay;xm; ygon/

6.2.1 Cryptographic Module \t&ntao;pEi xe;clyrrsm;

(Cryptographic Module Standards and Controls)

MOSS CA on pepvjclrltwu Key Generate jylvyjci;Ei Key Storage twu FIPS 140-1 (Level-3) tqi&on Hardware Security Module u to;jylygon/

6.2.2 Private Key u vtrsm;xe;clyr (Private Key (m out of n) Multi-Person Control)

jyXme;xm;jci;r&yg/

6.2.3 Private Key Escrow jylvyjci; (Private Key Escrow)

jyXme;xm;jci;r&yg/

6.2.4 Private Key Backup jylvyjci; (Private Key Backup)

MOSS CA on 4i;\ Private Key u obm0ab;tE&m,usa&mujy;aomtcg vyie; quvuaqmi&uEi&e (Recovery jylvy&e) twuom þ CP ygowrwcsursm;twi; Backup Copy xm;&ygon/ x Key rsm;u v0uu' (Encrypt) jylvyí HSM wi xnoi;jy; Disaster Recovery Site wwi or;qn;xm;&ygon/

6.2.5 Private Key rwwr;a[mi;xm;&r (Private Key Archival)

MOSS CA Key Pair rsm;ouwr;ueq;ygu ten;q;ouwr; (5) Ep rwwr;a[mi;tjzp or;qn;xm;&ygon/ x Key Pair rsm;u jyevno;pjci; rjylvyEi&e vtyaom Procedural Control rsm;xm;&ly; HSM wior;qn;xm;&ygon/ rwwr;a[mi;tjzpor;qn;xm;onouwr; (5) Ep ausmom;ygu þ CP wia&;om;xm;ontwi; vlcpmzsuq;ypygon/ ouwr;ueom; aom CA Certificate rsm;u ouwr;xyrrw;awmygu x Key Pair rsm;uo;í Sign x;jci;rjyl vyawmyg/

6.2.6 Private Key u Cryptographic Module xwi (o) Cryptographic Module r ajymi;a&ljci; (Private Key Transfer into or from a Cryptographic Module)

MOSS CA on rr\ Key Pair u vurwa&;x;jci;jy\vyrn Hardware Cryptographic Module wi Generate jy\vyygon/ ¤i;tjyi x Key Pair u Recovery jy\vy&etwu (Encrypt) jy\vyí rw\or;qn;xm;ygon/ x Key Pair u tjcm;aom Hardware Cryptographic Module o Backup tjzp ajymi;a&lygu Encrypt jy\vyxm;on ypjziom wpcrwpco ajymi;a&ljci;jy\vy ygon/

6.2.7 Private Key u v\0uu'ajymi;íor;qn;jci;

(Private Key Storage on Cryptographic Module)

Hardware Cryptographic Module (HSM) wi or;qn;xm;on MOSS CA \ Private Key u v\0uu'ajymi;xm;aom (Encrypted) ypjziom or;qn;xm;&ygon/

6.2.8 Private Key u Activation Data o;íumu,jci;

(Method of Activating Private Key)

MOSS CA on ¤i;\ Private Key q;&;jci;? c;,c&jci;? jy\yic&jci;? tcir&orm;r o;pjci;? zi\unjci;r&ap&e Activation Data u umu,jci;rm; jy\vyxm;ygon/

Private Key u to;jy\í Sign x;jci;jy\vyEi&e Activate jy\vy&mwi Trusted Person ten;q; (2) 0; yg0iy\vyrom atmijriaprn jzpygon/

Class 1 Private Key rm; ? Class 2 Private Key rm;Ei Class 3- Private Key rm;u umu,rjy\vy&etwu powrwc\urm- Subscriber to;jy\aom Workstation Ei Private Key u tjcm;orm; 0ia&muo;pjci;rjy\vyEi&e v tyaom &yyi;qi&mwm;q;umu,rrm; jy\vyxm;&ygon/ 4i;tjyi MOSS CA on Subscriber rm;tm; ty' (6.4.1) wi azmjyxm;ontwi; Password u to;jy\&e (o) tvm;wvjc\r&aponen;rm; to;jy\ygon/ (Private Key u to;jy\&e Password xm;&jci; ? Windows Login (or) Screen Saver Password (o\) Network Login Password rm;to;jy\jci;) rm;u jy\vyxm;ygon/

6.2.9 Private Key u Deactivation jy\vyjci; (Method of Deactivating Private Key)

MOSS CA on Signing vyie;jy\vyjy;aomtcgwi; Activate vyie;p0wi yg0icaom Trusted Person r Manual Shut Down jy\vyjci; ? Log Out jy\vyjci;jzi Private Key u Deactivate jy\vyygon/ ouaocvurw im;&r;o;porm;on rrvyie;aqmi&ujy;ontcgwi; CPS wi

azmjyxm;ontwi; rr Private Key u Deactivate vy&ewm0e&ygon/ RA Ei ouaocvurw im;&r;o;porsm;on rrvyie; aqmi&ujy;on tcgwi; rr Private Key u Deactivate vy&e ? e-Token u z, &m;jci; (o) Certificate Store & Key File rsm; zsucjci;wu jy|vy&ewm0e&ygon/

6.2.10 Private Key u zsuq;jci; (Method of Destroying Private Key)

MOSS CA on 4i;\ Private Key u zsuq;&mwi HSM u pu&xwrv tajctae (Factory Initial State)o ajymi;vjci;en;jzi jyevnwnaqmuo;pEijci;r&ap&e tlui;tuse r&atmi zsuq;ypygon/ xozsuq;ypontcgwi;rwwr; Log zixm;&rwwr;wixm;ygon/

6.3. Key Pair prxe;or;jci;Eiouqiaom tjcm;en;vr;rsm;

(Other Aspects of Key Pair Management)

6.3.1 Public Key tm;v;u rwwr;a[mi;xm;&r (Public Key Archival)

MOSS CA on 4i;\ Public Key Ei im;&r;o;porsm;\ Public Key tm;v;u rwwr;a[mi; (Archive) tjzp or;qn;xm;ygon/

6.3.2 ouaocvurwEi Key Pair to;jy|rumv

(Certificate Operational Periods and Key Pair Usage Periods)

MOSS CA Certificate \ Operational Period on y,zsujci;rc&ygu (3) Ep jzpygon/ xtjyi MOSS CA on ¤i;\ ouaocvurw ouwr;rueq;r (1) Ep lu|wií ouaoc vurwtop xway;jci;u &ypygon/

Certificate Issued to	Validity Period
End-user individual/organizational subscriber	Normally up to 1 year
CA/RA Administrator certificate	Normally up to 3 years

Table (3) – Certificate Operational Periods

6.4. Activation jy|vyjci; (Activation Data)

6.4.1 Activation Data jy|vyjci; Ei Installation jy|vyjci;

(Activation Data Generation and Installation)

im;&r;o;porsm;Ei MOSS CA wi yg0iorsm;on 4i;w\ Private Key rsm;twu Activation Data rsm;? Generate Ei Install jy|vy&mwi,i; Private Key aysmuq;? c;,? jyiqic&jci;? rqiorsm;r xwazmajymqjci;? o;pjci;wu umu,&een;vr;rsm;xm;&aqmi&u&rn/

Activation Data taejzi Password rsm;to;jy‖ci;Ei x Password rsm;u tv,wu ce re;jci;? c;,jci;rvyEi&e jy‖vyxm;&rn/ Activation Data rsm;uto;jy‖í Private Key u umu, xm;&rn/

6.4.2 Activation jy‖vy&mwi o;aomtc:utvursm;u umu,jci;

(Activation Data Protection)

im;&r;o;porsm;Ei MOSS CA \ ,lunpwc&aom0exr;rsm;on 4i;w\ Private Key rsm;twu Activation Data rsm;u en;vr;rsm;o;í ,i; Private Key aysmuq;jci; ? c;, ? jyiqic&jci; ? rqiorsm;r xwazmajymqjci; ? o;pjci;wu umu,xm;&&rn/

6.4.3 Activation jy‖vy&mwi o;aomtc:utvursm;Ei ouqiaom tjcm;talumi;

t&mrsm; (Other Aspects of Activation Data)

6.4.3.1 Activation jy‖vy&mwi o;aomtc:utvursm;ay;yjci;

(Acitvation Data Transmission)

Private Key \ Activation jy‖vy&mwi to;jy‖aom Data u ay;y&mwi aysmuq;jci; ? c;,c&jci; ? jy‖yic&jci; ? tcir&bzi[ajymqjci; (Disclosure) ? w&m;r0i to;jy‖jci; (Unauthorized Use) rc&ap&e umu,&rn/ Window Ei Network Logon User Name Ei Password u wzuí im;&r;o;porsm;\ Activation Data tjzpto;jy&mwi Network rwqiay;y‖aom Password u rouqiaom User rsm;rto;jy‖jci;r&ap&e umu,&rn/

6.4.3.2 Activation jy‖vy&mwi o;aomtc:utvursm;zsuq;jci;

(Activation Data Destruction)

Activation Data rsm;uto;jy‖í Private Key u aysmuq;jci;? c;,c&jci;? jy‖yic&jci;? tcir&bzi[ajymqjci; (Disclosure)? w&m;r0i to;jy‖jci; (Unauthorized Use) r&ap&epraqmi &uxm;yg‖on/ Activation Data rsm;u rwwr;xe;or;xm;onumvausmveí zsuq;ontcg Overwriting jy‖vyjci; (o) trewu,zsuq;ypjci; en; (2) rs‖;v; (o) wprs‖;rs‖;uo;í pepwus zsuq;yg‖on/

6.5 uey‖swmpepvjcla&; xe;cs‖yrrsm; (Computer Security Controls)

MOSS CA Ei RA vyie;rsm;twu ,lunpwc&onpepu A[tzEilu;luyrtzw \ oabmwncsujzi owrwxm;on vjcla&;qi&m nelum;csursm;Eitn uunr&atmi aqmi&uxm;yg‖on/

6.5.1 uey\wmvjcla&;twu en;ynmqi&m o;jcm;vtyc\urm;

(Specific Computer Security Technical Requirements)

MOSS CA **on 4i;** CA Software **Ei** Data File **rsm;u rouqiorsm;r** Access **rjy\vyEi &e ,lunpwc\&on pepxm;&ygon/ xtjyi** Key Generate **jy\vyaom** Computer ? CA **vyie;rsm;Eiouqion** Database **rsm;?** Server **rsm;tm; wu&uuiw,o;pEiciu owrwxm;& on ,lunpwc\orsm;uom ciay;xm;jy;civaom** Business **ta\umi;jyc\uj ziom o;pcijy\yg on/** General Application User **rsm;twu** Production Server **wi** Account **rxm;&yg/**

MOSS CA **** Production Network **u tjcm;** Components **rsm;Eio;jcm;jzpap&e** (Logically Separated) **aqmi&uxm;ygon/** Network Access **uvn;umu,xm;ygon/** MOSS CA **on 4i;** Production Network **u twi;yi;** (Internal) **Ei tjyiyi;** (External) **us\;aus0ia&mujci; rjy\vyEi&eei** Firewall **u to;jy\íumu,xm;ygon/**

Password **Eipyv\0;í ten;q;** Character **ta&twuuvn;aumi;** ? Alphanumeric **Ei** Special Character **rsm; aygi;pyyg0i&evn;aumi;** ? Password **rsm;uajymi;vay;&rnumvuvn; aumi; owrwxm;ygon/**

RA Software **Ei** Data File **rsm;u ,lunpwc\&onpeptjzpaqmi&uxm;&jy; rouqio rsm;r 0ia&muto;rjy\Eiatmi en;ynmpm&i;ppjci;qi&m owrwc\ursm;? ty' (4.5.1) Ei tn aqmi&uxm;ygon/**

RA **rsm;on** Network **u twi;yi;** (Internal) **Ei tjyiyi;** (External) **us\;aus0ia&mujci; rjy\vyEi&eei** Firewall **u to;jy\íumu,xm;ygon/** Network Activities **rsm;\ oabmobm0** (Nature) **Ei** Source **uueowjci;rsm;uvn; praqmi&uxm;ygon/** RA **rsm;on** Password **to;jy\rEi pyv\0;í ten;q;** Character **ta&twuuvn;aumi;** ? Alphanumeric **Ei** Special Character **rsm; aygi;pyyg0i&evn;aumi;** ? Password **rsm;u ajymi;vay;&rn umvuvn;aumi; owrwxm;ygon/ im;&r;o;porsm;\ tc\utvursm; xe;or;xm;&aom** RA Database **rsm;tm; wu&uto;jyjci;u owrwxm;on ,lunpwc\orsm;uom ciay;xm;jy; xoo;p&ermvn; civaom ta\umi;jyc\u** (Business Reason) **&&rn jzpygon/**

6.5.2 ueywm vjcla&;tqitajctae **(Computer Security Rating)**

vtyovjyXme;ygon/

6.6 en;ynmqi&m jzpp0rsm;xe;cyr **(Life Cycle Technical Controls)**

vtyovjyXme;ygon/

6.7 Network vlcla&;qi&m xe;cslyrrsm; (Network Security Controls)

MOSS CA Ei RA on ¤i;\ vyie;rsm;tm;v;u rouqiorsm;r0ia&muí rormrrsm; rjylvyEi&e vlcpwc&on Network pepxm;&aqmi&uygon/ rouqiorsm;tm; lun&ci rjylaom Sensitive Information rsm;u tjyetveay;y&mwi Encrypt jylvyí aomvn;aumi; ? Digital Signature rsm;o;pí aomvn;aumi; ay;yygon/

6.8 tcseqi&mrwwr;wijci; (Time-Stamping)

ouaocvurwrsm;? CRL rsm;Ei tjcm;aom Revocation Database rwwr;rsm;wi vyaqmion tcseEiae&uu rwwr;xm;&ygon/ xuo tcseqi&mrwwr;rsm;jylvyjci; twu Cryptographic en;pep to;jy&e rv tyyg/

7. ouaocvurw ? CRL Ei OCSP qi&mrsm; (Certificate, CRL and OCSP Profiles)

7.1 ouaocvurwqi&m Profile (Certificate Profile)

MOSS CA \ Certificate rsm;on-

(a) ITU-T Recommendation X.509

(b) RFC 5280 : Internet X.509 Public Key Infrastructure Certificate Ei CRL Profile, April 2002 ("RFC 5280") wEi uunygon/

terq;tqitm;jzi X.509 ouaocvurwrsm;wi atmuazmjyygrsm;yg0iygon/

(1) Serial Number

(2) Signature Algorithm

(3) Issuer DN

(4) Valid From

(5) Valid To

(6) Subject DN

(7) Subject Public Key

(8) Signature

7.1.1 Version trwp0 (Version Number(s))

im;&r;o;porsm;twu xway;aom Certificate Versionrm X.509 Version (3) jzpygon/

7.1.2 ouaocvurw Extension rsm; (Certificate Extensions)

vtyovjyXme;ygon/

7.1.2.1 Key Usage &n&,curm; (Key Usage Purposes)

X.509 Version (3) ouaocvurwrm;wi RFC 5280 owrwcurm;twi; xnoi; xm;yon/ X.509 Certificate rm;\ Key Usage Extension u atmuazmjyyZ,m;wiazmjyxm;on twi; Set and Clear jy\vyyon/ Key Usage Extension Criticality Field u a,b,tm;jzi False [xnoi;xm;yon/

		CAs	Class 1 and Class 2 End-User Subscribers	Automated Administration tokens and Class 2-3 End-User Subscribers
Criticality		TRUE	FALSE	FALSE
0	digitalSignature	Clear	Set	Set
1	nonRepudiation	Clear	Clear	Clear
2	keyEncipherment	Clear	Set	Set
3	dataEncipherment	Clear	Clear	Clear
4	KeyAgreement	Clear	Clear	Clear
5	keyCertSign	Set	Clear	Clear
6	CRLSign	Set	Clear	Clear
7	encipherOnly	Clear	Clear	Clear
8	decipherOnly	Clear	Clear	Clear

Table (4) – Settings for Key Usage Extension

7.1.2.2 Certificate Policies Extension

vtyovjyXme;yon/

7.1.2.3 Subject Alternative Names

vtyovjyXme;yon/

7.1.2.4 Basics Constraints

CA \ X.509 Version (3) CA ouaocvurwrm;\ Basic Constraint Extension wi CA Field u True Set ay;xm;yon/

7.1.2.5 Extended Key Usage

vtyovjyXme;yon/

7.1.2.6 CRL Distribution Point

Relying Party rsm;r CA ouaocvurwrsm;\ tajctaeu ppaq;Ei&etwu End User Subscribers rsm;\ CRL Distribution Points Extension wi CRL File u www.moss.com.mm/download/moss.crl r download vyEiygon/

7.1.2.7 Authority Key Identifier

CA on im;&r;o;porsm;\ X.509 Version-3 ouaocvurwrsm;\ Authority Key Identifier Extension wi ouaocvurwu xway;aom CA \ Public Key u xnoi; azmjyxm;ygon/

7.1.2.8 Subject Key Identifier

CA on X.509 Version 3 ouaocvurwrsm;\ Subject Key Identifier Extension wi ouaocvurwuiaqmitwuxway;xm;aom Public Key u xnoi; azmjyxm;ygon/

7.1.3 Algorithm Object Identifiers

CA on Certificate rsm;u atmuazmjyyg Algorithm to;jyí Signing jyvyygon/ SHA-1 with RSA Encryption uto;jyygon/

7.1.4 trnay;yp (Name Forms)

CA onouaocvurwrsm;\ Issuer Ei Subject Distinguish Name wi ty' (3.1.1) wi azmjyxm;ontwi;jznoi;ygon/

7.1.5 ouaocvurwtrnay;jci;qi&m owrwcsu (Name Constraints)

MOSS CA on Anonymous Name rsm;ucirjyyg/trnrsm;on t"ym,&&rntjyi im;&r; o;po\trnEivn;ygwourl&&rn/ trnrsm;on Unique Distinguished Name (DN) jzp&ygrn/

7.1.6 ouaocvurw\r0g'qi&m u,pm;jylcsu (Certificate Policy Object Identifier)

Certificate Policy Extension uto;jyyguouaocvurwrsm;wi 4i;w\ trl;tpm;tvu ty' (1.2) wi azmjyxm;onEitn CP \ Object Identifier (OID) xnoi; azmjy ay;xm;ygon/

7.1.7 r0g'qi&m to;jyr (Usage of Policy Constraints Extension)

jyXme;xm;jci;r&yg/

7.1.8 r0g't&ntao;ypEia0g[m&t"ym,ziqcu

(Policy Qualifier Syntax and Semantics)

vtyovjyXme;ygon/

7.1.9 ouaocvurw\ta&;lu;aomr0g'qi&ma0g[m&t"ym,rsm;uaqmi&ujci;

(Processing Semantics for the Critical Certificate Policies Extension)

jyXme;xm;jci;r&yg/

7.2 CRL Profile

CRL wiatmuazmjyygZ,m;twi; Basic Field rsm;yg0iygon/

Field	Value or Value Constraint
Version	X.509 Version 2 CRLs.
Signature Algorithm	Algorithm used to sign the CRL: SHA-1 (or) MD5 in accordance with RFC 3279.
Issuer	Entity who has signed and issued the CRL.
Effective Date	Issue date of the CRL. CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued.
Revoked Certificate	Listing of revoked certificates, including the serial number of the revoked certificate and revocation date.

Table(5)- CRL Profile Basic Fields

7.2.1 Version Number (S)

CA on X.509 Version 2 CRLs rsm;u (Support) jyvyygon/

7.2.2 CRL and CRL Entry Extensions

jyXme;xm;jci;r&yg/

8. uunr&?r&pm&i;ppjci;Ei tjcm;tujzwrrsm;

(Compliance Audit and Other Assessment)

MOSS CA \vyie;aqmi&urypm;lu;luyrEiA[tzwoabmwnxm;on Security Ei Technical Guideline wiazmjyxm;on tcutvursm;twi; lu;luyrtzr vtyov

ppaq;r jy\vyrnjzpyg on/ Root CA Ei lu;luyrtzw\ Compliance Audit jy\vy&&rtay:wi rwní nelum;ontwi; jznqn;aqmi&uom;rn jzpyg on/

xtjyi CA on 4i;\ ,lunpwc\&aompepu aocmr&ap&etwu jyevnppaq;jci; Ei ppr;ppaq;jci;jy\vy&mwi ten;q; atmuygwyg0iyg on/

- vjcla&;Ei vyx;vyen;rm; jyevnpppjci; (vjcla&;qi&m pm&upmwr;rm; ? CP/CPS ? CA Eiouqiaomoabmwpmc\yrm;) ?
- MOSS CA onatmuygtajctaermjzpay:v\i4i;\pepupm&i;ppjci;jy\vy&rn/
  - CA \ pepEi Root CA \pm&i;ppjci;rm;wi owrwxm;aom prm;ei uunrr&onu aw&&jci; ?
  - rawmwqxcurrm; (o) c\;azmuc&rrm; jzpay:jci; ?
  - CA pep\ vjcla&; (o) Integrity u y\up;Eiac\&aom uprm;jzpay:jci; ?
- CA on vtyygu Risk Management u aqmi&u&rn/

8.1 tujzwrlurEe;Ei tajctae (Frequency and Circumtance of Assessment)

- Root CA on ouaocvurwxway;yici&o CA rm;u (1) Epwi (1) lur en;ynm qi&mpm&i;ppjci;jy\vyygon/
- pm&i;ppjci;rm;u lu;luyrtzrvucaom t&ntc\i;jyn0on pm&i;pptzrm;Ei ppaq;ygon/ pm&i;pptzwi vurw&pm&i;uiwp0;Ei Certified Information System Auditor wp0; yg&rnjzply; wp0;0;on 'p*spw,ouaocvurwrm;Ei ,i;wEi ywouaom toynm ? A[ow&ojzp&rn/
- CA rm;on rrpeptwi; Internal Audit u wpEpvli (2) lur ppaq;jci;jy\vyygon/

8.2 tm;en;c\u (o) vtyc\urm;ay:rwnívyaqmic\u

(Action Taken as a Result of Deficiency)

MOSS CA on pm&i;ppjci; ppaq;c\ut& vtyc\urm;? ›ci;c\uEi tm;en;c\urm; &ygu lu;luyrtzEi Root CA r nelum;ontwi; jznqn;aqmi&uygon/ ›ci;c\u ? tm;en;c\urm;tay:rwní ta&;,rn Action u MOSS CA \ prtyc\yrtzr q;jzwygon/ MOSS CA \tyc\yrwi wm0e&orm;on Corrective Action Plan u taumitxnazm&e wm0e&ygon/ tu,í x›ci;c\uEivtyc\urm;on MOSS CA \ Security Ei Integrity u lcr;ajcmuxcuaprnqygu CA r Corrective Action Plan u &u (30) twi; a&;qí

oiavsmaomtcsetwi; taumitxnazmrnjzpygon/ Serious Exceptions r[won Deficiencies rsm;twu CA r xtcsu\ ta&;ygru wucsuí oiavsmaomta&;,ru q;jzwrn jzpygon/

9. tjcm;aomp;ym;a&;&mEi 0ya'qi&mtalumi;t&mrsm;

(Other Business and Legal Matters)

9.1 ay;oi;&rnialu; **(Fees)**

9.1.1 ouaocvurwxway;jci;Eiouwr;w;jci;twuay;oi;&rnai

(Certificate Issuance (or) Renewal Fees)

im;&r;o;porsm;r ouaocvurwxw,jci;? ouwr;w;jci;Ei ouaocvurwprce cjci;qi&mwtwu usoiaiu CA (o) RA rsm;olay;aqmi&ygrn/

9.1.2 ouaocvurwulun&jci;twu usoiai **(Certificate Access Fees)**

ouaocvurwrsm;tm; ouaocvurwrwwr;wu (Repository) wixnoi;jci; (o) Relying Party rsm;r to;jyEiatmiaqmi&uay;jci;wtwu usoiaiaumucrnr[wyg/

9.1.3 ouaocvurwy,zsupm&i;Ei tajctaeulun&jci;twuusoiai

(Revocation or Status Information Access Fees)

MOSS CA on Certificate Revocation List (CRL) xwjyejci;? x CRL u Relying Party rsm;r lun&Ei&ejyvyay;jci;wtwu usoiaiaumucrnr[wyg/ olaomtjcm;aom Value-Added Revocation Information 0eaqmirrsm;twu usoiaiaumucrnjzpygon/ CA on tjcm;aom Third Party rsm;r Revocation Information rsm;? Certificate Status Information rsm; (o) Repository wi Time Stamping jyvyjci;rsm;u CA r ouqi&mwm0ec\pmjzia&;om;cijy xm;jci;r&ygu cirjyyg/

9.1.4 tjcm;aom0eaqmirrsm;twuusoiai **(Fees for Other Services)**

MOSS CAon þ CP Ei ,i;Eiouqiaom CPS u Access vyjci;twuusoiai aumucjci; r&yg/ Document rsm;ulun&&r\ r[wb jyevnxwa0jci; (Reproduction) ? jyiqijci; (o) ,i;wu to;jyí tjcm;aomvyie;rsm; quvuvyuijci;uoaom tjcm;aom &n&,csursm;jzito;jyvygu Document rsm;u ryici (Copyright) &o MOSS CA Ei oabm wncsu &,aqmi&u&rn/

9.1.5 jyetr;aiay;jci;qi&m r0g'rsm; (Refund policy)

MOSS CA **on wi;usyaom vyx;vyen;rsm;** (Practices) **Ei r0g'rsm; csrwí ouaoc vurw xway;jci;qi&m vyie;rsm;u aqmi&uygon/ ouaocvurwxway;yici&or im;&r;o;potm; 4i;\ouaocvurwto;jy&mwi tqirajyr&ygu xw,jy; (7) &u twi; ,i;\vurwuy,zsuay;yg&e** MOSS CA **xo awmi;qvmaomtcg atmuygtwi; jyetr;aiu xway;ygon/**

- Class 3- Type-A **ouaocvurwwpapmivji**
  - **tp;&Xmeqi&mrsm;twu usy (15,000) jzpygon/**
  - **y*vuqi&mrsm;twu usy (20,000) jzpygon/**
- Class 3- Type-B **ouaocvurwwpapmivji**
  - **tp;&Xmeqi&mrsm;twu usy (10,000) jzpygon/**
  - **y*vuqi&mrsm;twu usy (20,000) jzpygon/**

9.2 b@ma&;qi&mwm0e,r (Financial Responsibility)

9.2.1 tmrcxm;&r (Insurance Coverage)

MOSS CA **on trm;rsm;Eicsevyxm;csursm;** (Errors and Omissions) **twu oiawmaom tmrcaiu tmrcurP (o)rru,yitptpOjzi tmrcxm;&ygon/**

9.2.2 tjcm;aom Assets rsm; (Other Assets)

MOSS CA **on ,i;\vyie;rsm;vyaqmi&e? wm0ersm;uaqmi&u&e? im;&r;o;porsm;Ei** Relying Party **rsm;tm; avsmalu;aiay;&e&ygu ay;acsEi&etwu vavmuaomaialu;&ygon/**

9.2.3 tjcm;aomtmrcwi yg0irrsm; (Extended Warranty Coverage)

jyXme;xm;jci;r&yg/

9.3. p;ym;a&;qi&m tcsutvursm;u v0ujci;

(Confidentiality of Business Information)

9.3.1 v0utjzpowrwxm;aom tcsutvursm; (Scope of Confidential Information)

MOSS CA **on im;&r;o;porsm;\atmuazmjyyg tcsutvursm;u v0utcsutvu rsm;** (Confidential and Private Information) **[owrwygon/**

- **ouaocvurwav0uxm;jci;qi&m tcsutvursm; Ei y;wwijycsursm; ?**

- Managed PKI u aqmi&uaeaom Customer rsm;\ Private Key rsm;?
- vyie;aqmi&urqi&mrwwr;rsm;tm;v;? pm&i;ppjci;qi&mrwwr;rsm; Eitp&icpmrsm;?
- Contingency Plan Ei Disaster Recovery Plan rsm;?
- Hardware, Software rsm;\vyie;aqmi&ur (Operation) \vjcla&;xe;cdyrrsm;? ouaoc vurw0eaqmiray;jci;\ vyie;prtycdyrqi&mrsm;Ei owrwxm;aom pm&i;a&;oi; jci;qi&m0eaqmirrsm;Ei ywouon tcutvursm;?

9.3.2 vW0utcutvursm;[rowrwxm;aom tcutvursm;

(Information not within the Scope of Confidential Information)

ouaocvurwrsm;? ouaocvurwy,zujci;Ei tjcm;ouaocvurw\tajctae (Status) qi&m owi;tcutvursm;? MOSS CA Repository Ei 4i;twi;& owi; tcutvursm;u vW0uEiy*lva&;qi&mtcutvursm; (Confidential and Private Information) tjzp rowrwy/ ty' (9.3.1) wi vW0u[owrwxm;aom tcursm;wi ryg0ionrsm;u vW0u&ervaom? y*lva&;qi&mr[waom tcutvursm; (Non-Confidential (o) Non-Private Information) [owrwygon/

9.3.3 vW0utcutvursm;uumu,&ewm0e,aqmi&ur

(Responsibility to Protect Confidential Information)

MOSS CA on tjcm;aomrouqiorsm; (Third Parties) r vW0uEiy*lva&;qi&m tcutvu (Confidential/ Private Information) rsm;u c;azmu0ia&mulun&jci; rjylvyEi&e praqmi&uxm;ygon/

9.4 wp0;wpa,muEiqionu,a&;tcutvursm;u vjcr&atmiaqmi&ujci;

(Privacy of Personal Information)

9.4.1 y*lva&;qi&m tcutvu vW0ujci;prcsu (Privacy Plan)

MOSS CA Ei RA rsm;on wp0;wpa,muEiqionu,a&;tcutvursm;u vjcr& atmi aqmi&u&etwu nelum;cursm;Ei uunr&aom Privacy Policy u a&;qaqmi&u xm;ygon/

9.4.2 u,a&;vW0utjzpourwontcutvursm; (Information Treated as Private)

ouaocvurwavmuxm;oEi ouqiontcutvursm;xr CA **r xway;on ouaocvurwrsm;? ouaocvurw** Directory **rsm;?** On-Line CRL **wi azmjyxm;onrsm;rví useaomtcutvutm;v;u u,a&;vW0utcursm;[owrwygon/**

9.4.3 u,a&;vW0ur[w[totrwjyxm;aom tcutvursm;

(Information Not Deemed Private)

trsm;jynolun&Eion ouaocvurwwiazmjyxm;on tcutvursm;u u,a&; vW0utcutvursm;[rowrwyg/

9.4.4 u,a&;vW0utcursm;u umu,&ewm0e,rrsm;

(Responsibility to Protect Private Information)

CA/RA **Ei 4i;** Participant **tm;v;on vuc&&xm;on vW0utcutvursm;u cs;azmulunc&jci;** (Compromise) **Ei tjcm;rouqiotztpn;rsm;x ay;yjci;^azmjyjci; rjzpap&e umu,xm;ontjyi w&m;p&iyicit& jynwi;& jyXme;xm;aom0ya'rsm;twi; uunr&ap&evn; aqmi&uxm;ygon/**

9.4.5 u,a&;tcutvursm;uto;jy&etwutalumi;lum;jci;Eioabmwncsu

(Notice and Consent to Use Private Information)

þ CP **wiyg&on u,a&;tcutvursm;u ouqion** Privacy Policy **(o) avmuxm; o\ oabmwncsur&&cvli to;jyrnr[wyg/ þ tyi;on** Privacy **qi&m umu,xm;&&rn owrwcsursm;twi; jzpygon/**

9.4.6 w&m;p&ia&; (o) prceca&;qi&mvyie;p0rsm;twuxwazmay;jci;

(Disclosure Pursuant to Judicial or Administrative Process)

MOSS CA **on rrxwi or;qn;xm;on** (Confidential) **Ei** Private Information **rsm;u prceca&;qi&muprsm;Ei tjcm;aomw&m;a&;qi&mvtyaomvyie;** (Legal Process) **rsm;twu lu;luyrtz\ cijycsujziom azmxwjyoci &ygon/**

9.4.7 tjcm;aomtcutvursm; xwazm&etajctaersm;

(Other Information Disclosure Circumstances)

jyXme;xm;jci;r&yg/

9.5 ÓPpr;&nyiqiciqi&m tcita&; (Intellectual Property Right)

MOSS CA on ouaocvurw im;&r;o;porsm;Ei Relying Party rsm;tm; ÓPpr;&nyiqiciqi&m tcita&;ay;jci; (IPR) (o) xojy(vyay;&e tcitmPmEiwm0er&yg/ þ CP ru;,aomrnontalumi;t&mrq þ CP ru;,alumi;u;um;cu?&nne;cuyg&&rn/

MOSS CA on atmuazmjyyg talumi;t&mwEi ywouí MOSS CA \ ryi[owrwygon/

- MOSS CA \ Hardware rsm; Ei MOSS CA r a&;om;xm;aom Manual rsm; ? av(muvmrsm;? &;wi;vyx; vyen;rsm;? MOSS CA Network layout rsm; ?
- þ CP Ei CPS ?
- CA \ trn Ei Internet Domain Name ?
- CA \ Key Pair rsm; ?

9.6 u,pm;jy(rrsm;Ei tmrcc:ursm; (Representations and Warranties)

9.6.1 MOSS CA rwm0e,rn tc:ursm; (CA Representations and Warranties)

MOSS CA ratmuyg tc:ursm;Ei pyv:0;í vavmuaomaocsmr&&rn/

- MOSS CA r xway;xm;aomouaocvurwav(muvmrsm; (o() xway;y;aom ouaocvurwrsm;r tc:utvursm;u rm;,i;pmazmjyjci; (Misrepresentation) r&&yg/
- ouaocvurwav(muxm;jci; (Certificate Application) (o) ouaocvurwjy(vy jci;wu praqmi&u&mü ouaocvurwr tc:utvu (Information) rsm;u ouaocvurw av(muxm;jci;u twnjy(o (o) ouaocvurw jy(vyo \ owc:W,i;ralumi trm;rsm;ryg&apyg/
- MOSS CA r xway;aomouaocvurwrsm;on þ CP Ei CPS wiyg&aom ? vtyaom owrwc:ursm;tm;v; (All Material Requirement) Ei uunr &ygon/
- ouaocvurwy,z:ujci;Eiqiaom 0eaqmirrsm; (Revocation Services) Ei Repository to;jy(ron þ CP Ei CPS rsm;& owrwc:ursm; (Material Aspects) tm;v;Ei uunr &ygon/

9.6.2 RA rwm0e,rn tc:ursm; (RA Representations and Warranties)

RA ratmuyg tc:ursm;Ei pyv:0;í vavmuaomaocsmr&&rn/

- ouaocvurwav(muvmrsm; (o) xway;y;aomouaocvurwrsm;r tc:utvu rsm;u rm;,i;pmazmjyjci; (Misrepresentation) r&&yg/

- ouaocvurwav\muxm;jci; (Certificate Application) (o) ouaocvurwjy\vy jci;wu praqmi&u&mü ,i;\azmjyygtcsutvu (Information) rsm;u av\muxm; jci;u twnjy\o (o) ouaocvurwjy\vyo\ owcsW,i;ra\umi trm;rsm; ry&ap&y/
- ouaocvurwrsm;on þ CP Ei CPS wiy&aom ? vtyaomowrwcsursm;tm;v; (All Material Requirement) Ei uunr&ygon/
- ouaocvurwy,zsujci;Eiqiaom 0eaqmirrsm; (Revocation Services) Ei Repository to;jy\ron þ CP Ei CPS rsm;&owrwcsursm; (Material Aspects) tm;v;Ei uunr &ygon/

9.6.3 ouaocvurwav\muxm;orwm0e,&rntcsursm;

(Subscriber Representation and Warranties)

ouaocvurwav\muxm;or tmrc&rntcsursm;rm -

- ouaocvurwwiyg0ion Public Key Ei 4i;Ei ouqiaom Private Key uo;í a&;x;xm;aom Digital Signature wi;onouaocvurwim;&r;o;po\ Digital Signature jzpon/ x Digital Signature uvurwa&;x;aecsewi4i; ouaocvurwon to;jy\í &aom taj\caewi&jy;ouwr;ueq;jci; (Expired) (o) y,zsuc&jci; (Revoked) taj\c taersl; rjzpap&yg/
- 4i;w\ Private Key uaocsmpmxe;or;umu,xm;&rn/ rnoncijy\rxm;aomo (Unauthorized Person) r ouaocvurwim;&r;o;po\ Private Key u,ío;pEijci; r&ap&yg/
- ouaocvurwav\muxm;oray;aomtcsutvursm;? ouaocvurw av\muvmwi a&;oi;aomtcsutvursm; Ei ouaocvurwwi azmjyxm;aom tcsutvursm;on reuer&&ygrn/
- ouaocvurwu þ CP Ei CPS wiy&on cijy\xm;aom? w&m;0iaom0ya'qi&m &n&,csursm; (Authorized and Legal Purpose) twuom to;jy\&ygrn/
- im;&r;o;poonrr\ouaocvurwtm; ouaocvurwxway;yici&o (CA) uo tjcm;aomouaocvurwrsm; ? CRL rsm;u vurwx;ay;jci; (Digitally Singing) rjy\vy &yg/

9.6.4 Relying Party rsm;rwm0e , rn tcsursm;

(Relying Party Representation and Warranties)

Relying Party **rsm;on rr , lunrjyton ouaocvurwEi 4i;wiyg0iaom ouaoc vurwqi&m tcsu tvursm;\ ppreru pO;pm;q;jzw&e v tyalumi;?** Relying Party Agreement **wia&;om;azmjycsursm;uem;vnygalumi;Ei ? , i;ouaocvurwu o;p&eoi ? roi q;jzw&e rrwiomwm0e&alumi; em;vno&&rnjzpygon/**

txupmy'wiazmjyxm;aom CP **yg** Relying Party **rsm;vuemaqmi&u&rnwm0ersm;** (Obligation) **u vuemrr&jci;alumi 0ya'qi&m tus;qursm;jzpay:vmygu , i;** Relying Party **r wm0e , vuc&rn jzpygon/** MOSS CA **\ , lunpwcspmo;porsm;\ oabmwncsu** (Relying Party Agreement) **wi tjcm;aom azmjycsursm;Ei tmrccsursm;uvn; xnoi;azmjyxm;ygon/**

9.6.5 tjcm;aomorsm;\ u , pm;jy rEi wm0e , rrsm;

(Representation and Warranties of other Paticipants)

jyXme;xm;jci;r&yg/

9.7 Warranties rsm;u jii;y , jci; (Disclaimers of Warranties)

wnq0ya'rsm;wicijy xm;on &n& , csursm;t& ouaocvurwo;porsm; oabmw ncsu (Subscriber Agreement) **Ei** Relying Party Agreement **rsm;on** MOSS CA **\ jzpEior** Warranties **tm;v;u (**Warranty of Merchantability **(o) &n& , csu wpctwu oiawmru tus;0iaom rnon** Warranty **rs;urq) jii;y , Eion/ xjyiaygqr** (Negligence) **or[w vucEiz , &aom owrjci;r&r** (Lack of Reasonable Care) **wtjyi** CRL **wi azmjyxm;aom qi;i ? y , zsujy;om;ouaocvurwrsm;tm; o;pjci;alumijzpay:vmaom tus;qursm;twu rnonay;&ewm0e** (Liability) **urq** MOSS CA **r jii;y , Eion/**

9.8 ay;&e&onrsm;u ueowxm;csursm; (Limitations of Liability)

MOSS CA **on ouaocvurwo;pralumi jzpay:on wu&u (o) wu&u r[waom** (Indirect) **? x;jcm;aom** (Special) **? tjypay;c&ralumijzpay:vmaom xcuq;&;rrsm;** (Punitive Damage) **? rawmwqjzpaom** (Incidental) **ponwalumijzpay:aom ysup;q;&;rrsm;u vn;aumi;? ppyrsm;Ei obm0ab;tE&m , rsm;alumi jzpay:aomysup;rrsm;twuvn;aumi; avsmalu;aiay;jci; rjy vyyg/** MOSS CA **r** Certificate **trs;tpm;tvu ysup;q;&;rtwu ay;avsmrrsm;** (Liabilities) **u trsm;q; atmuygtwi; owrwxm;ygon/**

Class	Liability
Class-3 (Type A)	- 60000 u:y
Class-3 (Type B)	- 30000 u:y

ouaocvurw im;&r;o;porm;\ Liability Ei Limitation u ouqi&mim;&r;o;porm; oabmwpmcdy (Subscriber Agreement) wivn;aumi;? Relying Party rm;\ Liability Ei Limit u Relying Party Agreement wivn;aumi; azmjyxm;ygon/

9.9 avmalu;aiay;jci; (Idemnities)

9.9.1 Indemnification by Subscribers

vtyov jyXme;ygon/

9.9.2 Indemnification by Relying Parties

vtyov jyXme;ygon/

9.10 pn;ur;cturm;Ei &ypjci; (Terms and Termination)

9.10.1 pn;ur;ctu (Term)

þ CP on MOSS CA \ Repository wi Publication jyvyonaerpí w&m;0i (Effective) ygon/ þ CP wi jyiqirrm;jyvyygu xjyiqirrm;on Repository wi Publish jyvyonaerpí tu;oua&mur &ygon/

9.10.2 &ypjci; (Termination)

rlumcP þ CP wi jyiqirrm;on Version topjyXme;jci;Ei ajymi;vr jyvyjci; r&oí w&m;0i CP jzpygon/

9.10.3 &ypjci;tu;w&m;rm;Ei vyie;quvu&ywnjci;

(Effect of Termination and Survival)

þ CP u&ypvuaomvn; CA \ Participant rm;on Certificate rm;\ Validity Period jynonwiatmi x CP ygtcurm;twi; tu;0ir&ygon/

9.11 wp0;ci;ptm;talumi;lum;jci;Eiquo,jci;

(Individual Notices and Communications with Participants)

vtyovjyXme;ygon/

9.12 jyiqirrsm; (Amendements)

9.12.1 jyiqirrsm;jyvyonvyx;vyen; (Procedure for Amendment)

þ CP wi jyiqirrsm;u CA Policy Management Authority r jyvyygon/ þ CP wi jyiqirwi;u lu;luyrtz\ twnjyc:u&,jy;rom jyiqijci; jyvyygon/ jyiqirrsm;u a&;om;xm;on Amended Form pm&uypjzi4i;? Update ypjzi4i;? &&Eiygon/ jyjyily;om; CP Version rsm; (o) Notices Section wivn; Link ay;xm;rn jzpygon/ þ CP wiajymi;vjci; jyvyrrsm;on CP Object Identifier rsm;wivn; ajymi;vrv? rvu MOSS CA Ei Root CA \ prtyc:yorsm;r q;jzwc:uay;ygon/

9.12.2 oway;talumi;lum;jci;en;vr;Ei umv (Notification Mechanism and Period)

MOSS CA on CP wi y&on pmyEyjci;qi&mtrm;rsm;? URL ajymi;vrrsm;? quo,&rn vypmajymi;vrrsm; ponwu lulwitalumi;lum;&eEi lu;luyrtz \ twnjyc:u&,&ew rvtyy jyjyiajymi;vci&on/ jyjyiajymi;vvonrsm;u tlujyc:u ay;yEi&etwu tc:eumvwpc owrwxm;ygon/ xjyjyiajymi;vrntc:ursm;Ei tlujyc:u rsm;u MOSS CA \ Website http://www.moss.com.mm wi azmjyxm;ygon/

9.12.3 OID ajymi;vjci;jyvyrn tajctaersm;

(Circumstances under which OID Must be Changed)

vtyovjyXme;ygon/

9.13 jyóemrsm;u ajz&i;rnen;vr;rsm; (Dispute Resolution Procedures)

MOSS CA Ei ouaocvurwim;&r;o;porsm;tlum; y#yursm;jzpym;vmygu 4i;wEi c:yqxm;aom oabmwnc:ursm;wi a&;om;xm;on Dispute Resolution Procedure rsm;twi; ajz&i;om;rn jzpygon/ vtyygu tvuxa&mep quo,aqmi&ua&;Oya'? ta&;ay:prrl Oya'rsm;ay:witajccí ay:ayguaomjyoemtwi;twmt& tvuxa&mepquo,aqmi&u a&; A[tz? lu;luyrtzEi quo,a&;nelum;rO;p;Xmew\ vr;nec:ursm;twi; ta&;, aqmi&uygon/

9.14 vr;r;on Oya' (Governing Law)

þ CP wi ziqxm;on twi; bmomjyejci; (Interpret) ? wnaqmujci; (Construction) ? tmPmwnapjci; (Enforceability) Ei w&m;0ijzpjci; (Validity) rsm;Eipyv:O;í

jrermEii\ wnq0ya'rsm;t&om aqmi&u&rn jzpygon/ jrermEii\ wnq0ya'rsm;omv\i þ CP u vr;r;on 0ya'jzpygon/

9.15 ouqion0ya'rsm;Ei uunr&jci; (Compliance with Applicable Law)

þ CP on jrermEiiawmtp;&r jyXme;xm;on 0ya'rsm;? ouqionen;0ya'rsm; (Regulations)? pn;rs0;rsm; (Rules)? trealumjimpmrsm;? nelum;csursm; Ei uunr&ygon/

9.16 taxax lu\wiprcsursm;tyi; (Miscellaneous Provisions)

9.16.1 oabmwncsutm;v; (Entire Agreement)

rouqiyg/

9.16.2 wm0eEi tcita&;rsm; xyqiay;tyjci; (Assigment)

þ CP wi yg0itus;0iorsm;on rrtm;ay;tyxm;on wm0eEi tcita&; rsm;u MOSS CA \ oabmwcijycsur&y vajymi; ay;tyjci;rjy\&/

9.16.3 0ya't&aqmi&uEir (Serverability)

þ CP ygazmjycsu (o) jyXme;csu ? pn;ur;csuwpcEi pyvs0;í ay:aygu v mon tajctaewp&ywi w&m;&;awm (Court of Law) (o) tjcm;aom c&;rsm;wiwijyu;um;jci;rjy\Ei caomvn; xazmjycsu (o) pn;ur;csurví þ CP \ usetpwtyi;rsm;on 0ya't& quvuí tus;oua&mur (Valid) &ygon/

9.16.4 tmPmoua&mujci; (u,pm;v,? a&\aetus;aqmicEi pevwo\ tcita&;)

Enforcement (Attorney's Fees and Waiver of Rights)

rouqiyg/

9.16.5 rwm;q;Eiaom? rveqeEiaomjzp&y (Force Majeure)

MOSS CA on obm0ab;tE&m,rsm;? ppab;pon wm;q;ír&Eiaomup&yrsm;alumi jzpay:vmaom ysup;q;&;rrsm;twu ay;avsm&ewm0er&yg/

9.17 tjcm;aom\ulwiprcsursm; (Other Provisions)

vtyov jyXme;ygon/

9.18 rwcsursm;ay;y&eumv (Comment Period)

þ CP Eipyvs0;ít lujycsu ? rwcsursm;ay;yvyguþ CP tm; Publish vyonaerpí (15) &utwi; MOSS CA o talumi;lum;pmay;yEiygon/ e-mail rm mossca@moss.com.mm jzpygon/

Table of Acronyms

aOg[m&	t"ym,owrwcsu
ARL	Authority Revocation List
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
FIPS	tar&uejynaxmip Federal Information Processing Standards
OID	Object Identification Value
LDAP	Light Weight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public-Key Infrastrature
Root CA	Root Certificatioin Authority
RA	Registration Authority
RSA	A Public Key Cryptographic System Invented by Rivest, Shamir, and Adelman
RFC	Request For Comment
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
MOSS CA	Myanmar Online Security Service Certification Authority

t"yg, owrwcsu

(u) ouaocvurw (Certificate) qonrm vurwa&;x;oEi x;jrvurw zew;aom tcsutvuw\ quE,ru aocsmapon tvuxa&mep tcsutvuowi;vm or[w tjcm;rwwr;tjzp ouaocvurwxway;ou im;&r;o;po (Subscriber) tm; xway;onvurwuqvon/

(or[w)

ouaocvurw (Certificate) qonrm ouaocvurwxway;yici&o (CA) \ Private Key jzia&;x;xm;aom 'p*spw, x;jrvurw (Digital Signature) jzi xway; xm;aom ouaocvurw im;&r;o;po (End Entity) \ Public Key Ei tjcm;aom tcsutvursm;yg0ion tcsutvuzpn;r (Data Structure) uqvon/

(c) rvt&i;tjrpouaocvurwxway;yici&o (Root Certificate Authority) qonrm ouaocvurwxway;yici&o (CA) rsm;o ouaocvurwrsm; xway;jci; ? prcecjci; ? y,zsujci; ? ouwr;w;jci;rsm;jylvyEi&e lu;luyrtzu tvuxa&mep quo, aqmi&ua&;0ya't& xway;onvipiu&&aom tztpn;u qvon/

(*) ouaocvurw xway;yici&o (Certificate Authority (CA)) qonrm tvuxa&mep x;jrvurwEi pyvs0;í 0eaqmirvyie; aqmi&uEi&e lu;luyrtzu tvuxa&mep quo,aqmi&ua&;0ya't& wm0eay;tyxm;aomy*lv or[w tzltpn;uqvon/

(or[w)

ouaocvurwxway;yici&o (Certificate Authority (CA)) qonrm Public Key Certificate rsm; jylvy&e ? xway;&eEi ,i;ouaocvurwrsm;\ ouwr;umv wavlmuv;twu wm0e,&e to;jylowp0; or[w trsm;r ,lun&aom tztpn;u qvon/

(C) ouaocvurway:vp (Certifice Policy (CP)) qonrm omrevjclrv tycsursm; Eitn tzltpn;wpc or[w to;cr tqitwe;wpc twu ouaoc vurwwpc to;jyEiru azmjyaom en;0ya' tptzu qvon/

(i) ouaocvurw xway;jci;qi&m vuemusio;&rn en;vr;rsm; (Certification Practice Statement (CPS)) qonrm ouaocvurwrsm;xway;&mwi ouaoc vurw xway;yici&o (CA) r to;jylon vuemusio;&rnen;vr;rsm; azmjycsu jzpon/

(p) ouaocvurwxway;yici&oy,zsupm&i; (Authority Revocation List (ARL)) qonrm rvt&i;tjrpouaocvurwxway;yici&o (Root CA) r vurwa&;x;í y,zsuxm;aom ouaocvurwy,zsupm&i;jzpon/ xouaocvurwy,zsupm&i; u trs;om;ouaocvurwrwwr;wu (National Repository) wi trsm;jyno tv, wuEi tcrlun&Ei&e azmjyxm;on/ ARL rsm;u tceqi&m rwwr;wijci; (Time Stamp) jylvyxm;ygon/

(q) ouaocvurwy,zsupm&i; (Certificate Revocation List (CRL)) qonrm ouaocvurw xway;yici&o (CA) r vurwa&;x;í y,zsuxm;aom ouaocvurwy,zsupm&i;jzpon/ xouaocvurwy,zsupm&i;u ouaoc

vurwrwwr;wu (Repository) wi trm;jyno tv,wuEi tcrlun&Ei&e azmjyxm;on/ CRL rm;u tcseqi&m rwwr;wijci; (Time Stamp) jylvyxm;ygon/

(Z) rwywixm;aom xway;yici&o (Registration Authority (RA)) qonrm ouaoc vurwavlmuxm;o\ talumi;t&mrm;Ei ywouí reuer&r& ppaq;jci; (Identification) Ei ouaocrppaq;jci; (Authentication) wtwu aqmi&uay;aom tzltpn;wpcjzpygon/ RA on ouaocvurwu vurwx;jci; or[w xway;jci;rjylyg/ (qvonrm RA wp0;on CA wp0;u,pm; wcslwm0erm;u aqmi &ujci;jzpon/)

(ps) ,lunpwcspmo;po (Relying Party) qonrm ouaocvurwu to;jylí ouaoc vurwEi 'p*spw,x;jrvurwrm;u ,lunpwcspmo;pou qvon/ þpmwr;wi ouaocvurwo;po (Certificate User) Ei ,lunpwcspmo;po (Relying Party) u tjyetveto;jylEion/

(n) ouaocvurwavlmuxm;o(o) im;&r;o;po (End Entity/ Subscriber) qonrm ouaocvurw xway;yici&o (CA) xr ouaocvurwwpcu awmi;qo jzpon/

(#) ouaocvurwouwr;w;jci; (Certificate Renewal) qonrm ouaocvurwwi yg0iaom Public Key or[w wjcm; tcsutvurm;u ajymi;vjci;r&b im;&r;o;po CA tm; ouaocvurwtopwpcxway;jci;jzpon/

(X) Key Pair topu to;jylí ouaocvurw ouwr;w;jci; (Certificate Rekey) qonrm Public Key topwpcuto;jylí ouaocvurwtopwpc xway;jci; jzpon/