Myanmar Online Security Service Certification Authority (MOSS CA)

ouaocvurw xway;jci;qi&m vuemusio;&rn en;vr;rsm;

(Certification Practice Statement)

aep/ 2012 cEp ! {jyv (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&m vuemusio;rn en;vr;rsm; (Certification Practice Statement (CPS)) u azmjya&;om;xm;aompmwr;jzpygon/ þpmwr;wi MOSS CA r ouaoc vurwo;porsm; (Subscribers) o ouaocvurwrsm; xway;jci;? ouwr;w;jci;? prcecjci;? y,zsujci;rsm; jy\vy&mwi vuemusio;rn MOSS CA \ ouaocvurwxway;jci;qi&m r0g'rsm; (Certificate Policies (CP)) yg owrwcsursm;Eitn to;jy\rnen;vr;rsm;u azmjyxm;yg on/

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

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;vyuicivipi&&cygon/ MOSS CA on ouaoc vurw im;&r;o;prnorsm;twu 'p*spw,ouaocvurwrsm; (Digital Certificates) u vurwa&;x; xway;ygon/ ,i;tjyi Certificate Life Cycle 0eaqmirrsm; (ouaoc vurwtop xway;jci; ? ouwr;w;jci; ? prcecjci; ? y,zsujci;) tm;v;uvn; aqmi&u ay;ygon/ MOSS CA \ ouaocvurwu Root CA r vurwa&;x;xway;ygon/ þ CPS wi ouaocvurw o;porsm;twu aqmi&uxm;rrsm; ? MOSS CA r ouaocvurw xway;&mwi vuemusio;rn en;vr;rsm;Ei ouaocvurwrwwr;wuaqmi&uxm;rrsm; yg0ijy;4i;u www.moss.com.mm wi Download jy\vy&,Eiygon/

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

ouaocvurw\ trsl;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;yoreuealumi;Ei tcsutvursm;\reueru o&Eiap&evn;aumi; to;jyEiygon/

1.2 CPS trnEi trwtom; (Document Name and Identification)

þpmwr;on MOSS CA \ CPS jzpygon/ þ CPS \ Object Identification Value (OID) rm (2.16.104.1.1.2.2) jzpygon/ þ OID u r0g'rsm;xyrowrw&e vtyygu w;csEiyg on/

1.3 PKI wiyg0iorsm; (PKI Participants)

1.3.1 A[tz

þ CPS 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 CPS 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&m taxmutuay;&e ? ouaocvurwxway;yici&o (CA) rsm;o ouaocvurwrsm; xway;jci; ? ouwr;w;jci; ? prcecjci; ? y,zujci;rsm;jy(vyEi&etwu tvuxa&mepquo,aqmi&ua&;0ya't& lu;luyrtzu trepmjzi wm0eay;cetyxm; 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 \ ouaocvurwu Root CA r vurwa&;x;xway;ygon/ im;&r;o;po (Subscriber) rsm;twu ouaocvurwu MOSS CA r pppxway;ygon/

Myanmar Online Security Service Co., Ltd. on tvuxa&mepquo,aqmi&ua&; A[tz\cijycsujzi lu;luyrtzr xway;xm;aom CA vyie;vipi &&xm;aom tztpn; jzpygon/

1.3.5 ouaocvurwim;&r;o;porsm; (Subscribers)

MOSS CA r xway;aom ouaocvurwuim;&r;o;potm; ouaocvurwim;&r;o;po (Subscriber) rsm;[ac:qygon/ ouaocvurwim;&r;o;po (Subscriber) rsm;on vwp0;csi;aomvn;aumi;? tzltpn;aomvn;aumi;? en;ynmqi&mypn;rsm;aomvn;aumi; jzpEiygon/

1.3.6 ouaocvurwu,lunpwcspmvuctojyforsm; (Relying Parties)

MOSS CA r xway;aomouaocvurwrsm;u ,lunpwcspm vuco;paomorsm;on Relying Party rsm;jzpygon/

xorsm;rm -

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

2/ MOSS CA Ei Cross-Certification jylvyxm;on Foreign CA rsm;\ ouaocvurwim;&r;o;porsm;?

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

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[wppaq;jci; (Identification) Ei avmuxm;orsm;tm; ouaocrppaq;jci; (Authentication) wtwu wm0e,aqmi&uay;aom vy*v (or[w) tzltpn;wpc jzpygon/ (qvonrm RA on CA u,pm; reuer&? r& ppaq;jci; (Identification) Ei ouaocr ppaq;jci; (Authentication) wm0ersm;u aqmi&uay;ygon/)

1.3.8 ouaocvurw rwwr;wu (Repository of Digital Certificates)

ouaocvurw rwwr;wuqonrm MOSS CA rxway;xm;aomouaocvurw tm;v;Ei ouaocvurwy,zupm&i;rsm;u trsm;jynortcsera&;0ia&mulun&Ei&e or; qn;rwwr;wixm;on MOSS CA \ouaocvurwrwwr;wujzpygon/ xrwwr;wuu (24) em& ? (7) &uywv; (Internet quo,rjywawmuaecservi) 0ia&mulun&Eiatmi praqmi &uxm;ygon/

1.3.9 CPS oiawmto;0ir (Applicability)

þ CPS on MOSS CA rxway;on ouaocvurwtm;v;Ei ouqiygon/ þ CPS & vyx;vyen;rsm; ? vuemusio;rnen;vr;rsm; (Practices) tm;v;on MOSS CA r ouaocvurwim;&r;o;porsm;o xway;xm;on ouaocvurwEi ouaocvurw y,zupm&i; (Certificate Revocation List (CRL)) rsm;u to;jyjci;rsm;? ouaocvurw ouwr;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;tm; xway;aom ouaocvurwrsm;u

- 'p*spw,vurwa&;x;&e (Sign)?
- E-mail u vW0uu'ajymi;í ay;yEi&e (Encrypt)?
- ay;yaom tcsutvursm;u r&i;pmtwi; ajymi;vzw&&e (Decrypt)?
- E-mail ay;yo rnorn0gpprealumi; taxmutxm;tjzpto;jy&e (Prove Identity)?
- Code Signing jyvvy&e Ei
- Server 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; ? CP ? þ CPS wEi uunr &cvi to;jyEiygon/ ouaocvurw trs;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&muav\muxm;&ervb** e-mail **jzi** Online **av\muxm;orsm;uxway;aom ouaocvurwtrsm;tpm; jzpygon/**

Class 2 Certificate

Class 2 **trsm;tpm;ouaocvurwu avsmuxm;or vtyaomtaxmutxm; pm&upmwr;rsm; Eiwu av\muxm;&rnjzpygon/ vu,wivma&muav\muxm;&ervyg/**

Class 3 Certificate

Class 3 trsm;tpm;ouaocvurwu avsmuxm;or vtyaomtaxmutxm;pm&upmwr; rsm;Ei av\muxm;ou,wir vma&muav\muxm;jci; ? xw,jci; jy\vy&ygrn/ vtyaom taxmutxm;rsm;wi ten;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&rtqieraomouaocvurwtrs;tpm;jzpygon/ xouaocvurwtm; Authentication jyvy&eEi Non-Repudiation uaxmuyay;&e &n&,curm;jzitо;rjyoiyg/ þouaocvurwon im;&r;o;po\ u,a&;tcutvu rm; (Identity) u ouaoc&mwi to;rjyEiyg/ Relying Party rim;&r;o;po\ ouaocvurwu to;jyí tcutvurm;u v0uuwtjzp ajymi;vEiaomvn; vucoon ouaoc vurwyiqioppreaumi;aocmrr&Eiyg/

Medium Assurance Level : ,lunpwc&rtv,tvwtqi (Medium) &aom ouaocvurwtrs;tpm;jzpygon/ þouaocvurwu tztpn;twi;Ei p;ym;a&; qi&mrm; ? t;ar;vto;jyrwi im;&r;o;po\ u,a&;tcutvurm; (Identity) u ,lun pwc&rtv,tvwtqi (Medium) vtyaomtcgrm;wi to;jy&eoiavmygon/

High Assurance Level : ,lunpwc&rtqijriaom ouaocvurwtrs;tpm;jzpygon/ im;&r;o;po\ u,a&;tcutvurm; (Identity) \ ,lunpwc&rtqirm ouaocvurw trs;tpm; Class 1Ei Class 2 xuyí jriygon/

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

tvuxa&mep quo,aqmi&ua&;Oya' ? ,i;Eiouqion en;Oya'rm;Ei tre alumjimpmrm;wi cijyxm;ontwi; ? ouaocvurwwi cijyxm;aomcijycut&om ouaocvurwrm;u to;jy&rn/ vuxcu'gP&m &apEiaom ? aoq;apEiaom (o) obm0 yw0e;usiu xcuysup;aponpeprm;\ xe;cyru&,mrm;wi ouaocvurwu xe;cy&e &n&,cujzi to;rjy&yg/ MOSS CA \ ouaocvurwu im;&r;o;porm; (Subscriber) o vurwxway;jci; ? CRL Sign x;jci;vyie;rm; pon CA vyie;rm;rví tjcm;aom aqmi&urrm;twu to;rjyyg/ Subscriber twu xway;aom ouaocvurwu CA Certificate tjzp to;rjy&yg/ Class-1 Certificate rm;u ouaocvurwuiaqmi o\ wn&rouaojy&e (Proof of Identity) Ei aqmi&urrm;u jii;qjci;rjyvyEi&e (non repudiation) &n&,curm;twu to;rjy&yg/

1.5 ouaocvurwxway;jci;qi&m r0g'rsm; prcelcjci; (Policy Administration)

1.5.1 CP/CPS tm; prftycsya&;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

Attension- 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 CP Ei þ CPS \ oiavsmrEi to;0iru q;jzwygon/

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

þ CPS 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; CPS \ e*rv ReferenceVersion & &n&,xm;on (Designated) (o) qeusirrsm; (Conflicts) u ae&m,^vr;r;r &ygon/ þ CPS wi jyiqiralumi CP wi jyiqi&evtyygu Root CA xwijyjy; cijycsujzi aqmi&uygon/

1.6 t"yg,owrwcsuEi twausmupmv;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)

MOSS CA on trsm;jynorouaocvurwrsm;u 0ia&mulun&eirn Online ouaocvurwrwwr;wu (Repository) xm;&ygon/ MOSS CA r xway;xm;aom ouaocvurwrsm;Ei zsuor;xm;aom ouaocvurwrsm; (CRL) u ,i;rwwr;wuwi trsm;jyno lun&Ei&etvim xwa0azmjyay;xm;ygon/ xtjyi ouaocvurw u ,lunpmvucto;jyorsm; (Relying Party) r ouaocvurw\ tajctae (Certificate Status) Eiywouaom tcsutvursm;u MOSS CA \ Website jzpaom (www.moss.com.mm) wi owi;tcsutvursm;uvn; 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) Eiywouaom tajctaersm;u lun&Ei&e ? ouaoc vurwu ,lunpmvucto;jylo (Relying Parties) rsm; Download jylvyEi&e Web-Based ouaocvurw rwwr;wu (Repository) xm;&ygon/ xtjyi OCSP (Online Certificate Status Protocol) 0eaqmir (&ygu) to;jyl í 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 wi tcsejynazmjyxm;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;jylr User Manual rsm; ?

ouaocvurwrsm;u atmuazmjyygtwi; xwa0 (Publish) ygon/

Certificate Type ouaocvurwtrs;tpm;	Publication Requirement Publication vtycsu
Root CA \ ouaocvurw	Relying Partyrsm;r lun&Ei&e MOSS CA \ Repository jzpon http://www.moss.com.mm/ Repository wi xwjyexm;ygon/
MOSS CA \ ouaocvurw	http://www.moss.com.mm wi Download jylvyEi&e xwjyeay;xm;ygon/
ouaocvurwuiaqmio (Subscriber) rsm;\ ouaocvurwrsm;	MOSS CA \ WebSite http://www.moss.com.mm wi &&Eiygon/

Table (2) - Authentication of Individual Identity

2.3 yEyxwa0rntlurEitcse (Time or Frequency of Publication)

MOSS CA r xway;xm;aomouaocvurwrsm;Ei ouaocvurwy,zsupm&i; (CRL) rsm;u ouaocvurwxway;jci; ? y,zsujci;jylvyontcgwi; Website wi xwjyeay;rn/ tu,í CRL wiazmjyxm;aom ouaocvurwrm ouwr;ueq;om;ygu xouaocvurw ouwr;ueq;y;aemuyi; xwjyexm;aom CRL rsm;wi ¤i;u xnoi; vrrnr[wyg/

Subscriber Agreement Ei Relying Party Agreement rsm;wi jyiqirrsm;u jyiqirjylvyontcgwi; xwjyeay;ygrn/ CPS wi jyljyirrsm;u þ CPS \ ty' (9.12) wi azmjyxm;ontwi; aqmi&uygon/

2.4 ouaocvurw rwwr;wu& tcsutvursm;xe;csyr

(Access Controls on Respository)

MOSS CA on ouaocvurwrwwr;wu& tcsutvu (data) rsm;tm; vyyicir&aomy*lvrsm;r xyrjznpujci; ? zsujci; ? jyljyijci;rsm; rlyvyEi&e vtyaom umu,xe;csyrtptr (control) rsm; jylvyxm;ygon/ ouaocvurw rwwr;wutm; 0ia&mulun&jci;u ueowxm;jci;r&yg/ ouaocvurwrsm; ? ouaocvurwtajctae qi&m tcsutvursm;Ei CRL u 0ia&mulun&Ei&e Relying Party Agreement (RPA) u oabmwn&rn jzpygon/

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

3.1 trnay;jci; (Naming)

3.1.1 trn tr;tpm;rm; (Type of Names)

MOSS CA ouaocvurw\ Issuer Ei Subject Field rm;wi X.501 Distinguished Name (DN) rm;yg0iyg on/ Distinguished Name (DN) wiatmuazmjyyg Z,m;twi; tpwtyi;rm; yg0iyg on/

Attribute	web; (Value)
Country (C) =	Eiitrn (e.g. mm)
Organization (O) =	Myanmar Online Security Service Co. Ltd.
Organization Unit (OU) =	Myanmar Online Security Service CA
State or Province (S) =	Yangon
Locality (L) =	Yangon
Common Name (CN) =	Myanmar Online Security Service SHA256 CA
E-mail Address (E) =	mossca@moss.com.mm

Table (3) – Distinguished Name Attributes in CA Certificates

ouaocvurwim;&r;o;porm;\ Subject Name Field \ X. 501 Distinguished Name wi tpwtyi;rm; atmuazmjyygZ,m;twi; yg&yg on/

Attribute	Value
Country (C) =	Eiitrn (e.g. mm)
Organization (O) =	atmuyg twi;to;jyyg on/ Web Server Certificate rm;twu im;&r;o;po\ Domain trnu o;pyg on/ Individual certificate rm;wi urP&yg u xnoi;&e/ r&yg u uuvyxm;&e/ Oyrm- Myanmar Online Security Service Co., Ltd.
Organization Unit (OU) =	MOSS CA \ Certificate u im;&r;o;porm; \ Certificate wi OU Attribute rm;pmyg0iEiyg on/ • im;&r;o;po\Xmetrn (&yg u) Oyrm- MOSS CA
State or Province (S) =	im;&r;o;poaexion jyne,^wi;trn Oyrm- Yangon
Locality (L) =	Irwe,^&yuuvypm xnvyguxn&e Oyrm- Yangon

Common Name (CN) =	þ Attribute wi - Domain Name (for Web Server Certificates) - Organization Name/ User Name (for Code / Object Signing Certificates) - Name (for individual certificates). Oyrm- Aung Aung
E-mail Address (E) =	im;&r;o;po\ e-mail vypm e.g. aungaung@mptmail.net.mm

Table (4) – Distinguished Name Attributes in End User Subscriber Certificates

ouaocvurw im;&r;o;powi;on ujym;jcm;em;&i;vi;í wpcwn;jzpaom X.501 Distinguished Name (DN) wpc ouaocvurw\ Subject Name wi y&yon/

3.1.2 trnrsm; t"yg,jyn0ap&ev tyjci; (Need for Name to be Meaningful)

ouaocvurwim;&r;o;porsm;on ouaocvurwrsm;\ Subject Field wiyg0irn trnrsm;u em;vn&ev,uon? trsm;o&aom &i;vi;aom ? t"yg,&on ?4i;w\ wn&ru q;jzway;&e trnrsm;u to;jy&rn/

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

(Anonymity or Pseudonymity of Subscribers)

MOSS CA on ouaocvurwim;&r;o;p&e avmuxm;orsm;tm; rr (o) tztpn; \ trnrsm;u emrn&i; r[won tjcm;aom trnrsm; xm;&o;pcirjyyg/

3.1.4 trnrsm;u bmomjyern pn;rsO;rsm; (Rules for Interpreting Various Name Forms)

jyXme;xm;lci;r&yg/

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

ouaocvurw im;&r;o;porsm;\ Subject Distinguished Name rsm;on MOSS CA \ Domain twi;wi wprsl;wn; (Unique) jzp&rn/

3.1.6 to trwjyjci;? ppreaumi;xi&m;apjci;Ei ueypn;trwtom;rsm;\ tce;u@

(Recognition, Authentication and Role of Trademarks)

MOSS CA on ouaocvurwav|muxm;orsm;tm; tjcm;orsm;\ ÓPpr;&n yiqirqi&m tcita&; (Intellectual Property Right (IPR)) u us;verjzpapon trnrsm;o;p av|muxm;jci; cirjyyg/ av|muxm;orsm;on tjcm;orsm;\ IPR u azmuzsujci;&^r&u MOSS CA r ppaq;jci; rjy|vyyg/ tu,í xotjii;ym;rrsm; ay:ayguvmygu MOSS CA on xo\ouaocvurw av|muxm;jci;Ei ouaocvurwwu y,zsuEion (o) qi;ixm; yici&on/

3.2 ue0; rnorn0gjzpalumi; ppaq;jci; (Initial Identity Validation

3.2.1 Private Key yiqialumi;ouaojyrnen;vr;

(Method to Prove Possession of Private Key)

ouaocvurwav|muxm;oon ouaocvurwxw&mwi to;jy|rn Private Key on ¤i;yiqilci; reuealumi; ouaojy&rn/ xoouaojy&mwi PKCS#10 File (o) tjcm;aom ¤i;uoaom Cyrptographic en;vr;rsm; (o) MOSS CA r oabmwxm;on en;vr;rsm;jzi ouaojyEiygon/ MOSS CA r im;&r;o;pou,pm; Key rsm; Generate jy|vyay;ygu þvtycsuon 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;or ay;aom av|muxm;ryg tjcm;tcsursm; (ppaq;&e rvtyon tcsursm;rví) reuer&alumi;u MOSS CA \ rwywijci;qi&mvyie;rsm; aqmi&uaom tztpn; (RA) r Document ppaq;on en;vr;rsm;twi; ppaq; twnjyyg 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&ru tmrcEion tmPmyitztpn; wpcc \ pm&upmwr;?axmuccsursm;u ppaq;jci;rsm; jy|vyygrn/
- ouaocvurwav|muxm;otm; ,i;tztpn;r cijycsujzi av|muxm;jci;jzp alumi;? tztpn;r o&alumi;u w,vze; (o) pm (o) tjcm;aom en;vr;rsm;uo;í ppaq; twnjyygon/ 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;yg0iyu ouaocvurw av|muxm;oon x Domain Name u o;pciEi E-mail Domain Name u o;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;uv tyygu jy|vy om;rn jzpygon/

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

ouaocvurw av|muxm;o wp0;wpa,muc\i;p\ Identity ppaq;jci;u ouaocvurw trs\;tpm;tvu jy|vyygrn/ av|muxm;ou terq;tm;jzi Eiiom;pppa&; u'jym; (o) rwywiu' (o) Eiiu;vurwEi wuqippaq;jci;rsm; |yvyygrn/

ouaocvurwim;&r;o;pot m;ppaq;jci;jy|vyrn tc\ursm; (Authentication Standard) u ouaocvurw trs\;tpm;tvu atmuygZ,m;wi azmjyxm;ygon/

ouaocvu rwtrs\;tpm;	ppaq;rnen;vr;
Class – 1	ppaq;rrjy|vyyg/ oaom ouaocvurwav|muxm;o\ E-mail jzi jye|um;c\u (Reply) vuc&&rom ouaocvurw xway;ygrn/
Class-2	ouaocvurw av|muxm;or ay;aom tc\utvursm;u MOSS CA (o) RA r vucaom rwwr;rsm; (Database) or;qn;xm;ontztpn;rsm; (o) p;ym;a&; qi&mrwwr;rsm;? vr;nepmtyrsm;? 0exr;pm&i;rsm;^rwwr;rsm; (o) Database rsm;& tc\utvursm;Ei wuqippaq;jci;rsm; jy|vyygon/
Class-3	Class-3 Certificate ppaq;jci;u av|muxm;ou,wi MOSS CA \ RA a&armuo vu,wivma&muapjci;jzi ppaq;ygon/ av|muxm;ou Eiiom; pppa&; u'jym; (o) rwywiu'&"gwy (o) Eiiu;vurw& "gwyEi wuqi ppaq;jci; rsm; jy|vyygon/

Table (5)- Authentication of individual identity

3.2.4 tcsi;csi;vyie;vyaqmiEir&&etwu ourwcsursm;

(Criteria For Interoperation)

jyXme;xm;jci;r&yg/

3.3 ouwr;w;&eavmuxm;rrsm;u reuer&?r& ppaq;jci;Ei ouaocrppaq;jci;

(Identification and Authentication for Re-Key Request)

'p*spw,ouaocvurwrsm;ouwr;rueq;rouaocvurwto;jyjci; jywawmurl r&ap&etwu ouaocvurwtopwpc &&&evtyygon/ ouaocvurwrsm;tm;v; ouwr;w;ontcg ty' (4.2) twi;ppaq;í ouwr;ueq;rn ouaocvurwlae&mwi tpm;x;&etwu ouaocvurwtopwpcu MOSS CA r xway;ygon/

3.3.1 yreouwr;w; (Re-Key) rsm;uppaq;jci;Ei twnjyjci;

(Identification and Authentication for Routine Re-Key)

ouaocvurw ouwr;w;jci; (Re-Key) rjyvyr Re-Key avmuxm;jci;jyvyo ? vy*v (o) tztpn;on xouaocvurwuiaqmio (Subscriber) tpptrejzpalumi; ty' (4.6) yg owrwcsursm;twi;ppaq;ygon/

ouaocvurwtrs;tpm; (Class 1) twu ouwr;w;jci; vucrnen;vr;wpcrm Challenge Phrase (o) tvm;wwpcc (o) Private Key yiqialumi; ouaojyjci;wjzi ouwr;w; avmuxm;jci;uvucjci;jzpygon/ ouaocvurwouwr;w;jci; aqmi&u&m wi ouwr;w;avmuxm;oon 4i;l Challenge Phrase (o) tvm;wu reuepmjznpuay;Ei? ajymEiontjyi ouwr;w;avmu&mwi jznoi;ontcsursm;Ei ue0;ouaocvurw avmuxm;&mwi jznoi;ontcsutvursm; (aumy&wEi Technical Contact Information rsm; tygt0i) ujym;r ? ajymi;vrr&ygu ouwr;w;ouaocvurwtopu xway;rnjzpygon/

Rekey (o) Renewal jyvvy&eawmi;qontcgwi; MOSS CA on ouaocvurw im;&r;o;po avmuxm;p0u to;jylon ppaq;onen;vr;rsm; ? ouaocrppaq;jci; jyvvyon en;rsm;twi; jyevnppaq;ygon/

3.3.2 ouaocvurwy,zsuly;aemu ouwr;w; (Re-Key) jyvvy&e avmuxm;jci; rsm;u pprealumi;ppaq;jci;Ei reuealumi;twnjyjci;

(Identification and Authentication for Re-Key After Revocation)

atmuazmjyygtalumi;rsm;alumi ouaocvurwuy,zsuc&ly;aemu ouwr;w; (Re-key Ei Renewal) iyvy&e avmuxm;vmjci;rsm;u cijylrnr[wyg/

- ouaocvurwrsm; (Class-1 Certificate rvíi) MOSS CA (o) RA \ w&m;0icijycsur&&y ouaocvurwxway;xm;jci;alumi y,zsuc&cv\i?
- ouaocvurwav\muxm;o\ vurwav\muxm;jci;qi&mtcsursm;u twn iyay;or av\muxm;csuyg tcsursm;on rm;,i;azmjyon (o) rm;,i;aealumi; us;alumi;civpmo&í ouaocvurwy,zsuc&cv\i?
- MOSS CA Ei ,i;\vyie;rsm;u umu,apmia&mu&etwu tjcm;aom talumi;jycsuuprsm;alumi y,zsujci;c&cv\i?

3.4 ouaocvurwy,zsu&e awmi;qjci;twu ppaq;jci;Eitwnjy\ci;

(Identification and Authentication for Revocation Request)

rnonouaocvurwurq y,zsujci;rjy\r ouaocvurwy,zsu&e MOSS CA Ei ouaocvurwav\muxm;ou,wir awmi;qjci;[w?r[wu aocsmpm ppaq;íq;jzwygon/ ouaocvurwuiaqmior y,zsuay;&e awmi;q?av\muxm;jci;rsm;u ppaq;twnjy\ (Authentication) aom vyx;vyen;rsm;wi atmuygtcsursm;yg0ion/

- wpcsWaom ouaocvurw trs;tpm;rsm;wi y,zsu&eav\muxm;oonouaocvurwuiaqmio\ Challenge Phrase vW0upum;p (o) tvm;wpum;pjzi av\muxm;y;xpum;ponrwwr;xe;or;xm;aompum;pEiwnv\iouaocvurwuy,zsuay;jci;?
- im;&r;o;por ouaocvurwy,zsu&e (Revoke) awmi;qonav\muvmu 4i;r 'p*spw,vurwa&;x;íav\muxm;y; x'p*spw,w,vurwonvn; reuev\i y,zsuay;jci;?
- ouaocvurwav\muxm;ox quo,talumi;lum;í y,zsu&eawmi;qoon ouaocvurwuiaqmiou,wijzpalumi; aocsmapjci;?(xoquo,&mwi tajc taeay:wirwní Phone? Fax? E-mail? Courier Service rsm;u to;jy\Eiygon)/

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

4. ouaocvurw Life-Cycle vyie;aqmi&ur v tyc\ursm;

(Certificate Life-Cycle Operational Requirements)

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

ouaocvurwo;p&e av\muxm;vyg u taqmi (17)? ajrnxy? MICT Park? wuovrsm;vie,ajr ? &euejr\& MOSS Sale Office RA xo quo,av\muxm;Eiyg on/ av\muvmypu MOSS CA \ Website jzpaom www.moss.com.mm wi Download jy\vyí jznpuav\muxm;Eiyg on/

4.1.1 ouaocvurwav\muxm;ci&orsm; (Who Can Submit a Certificate Application?)

atmuyg tc\ursm;Ei uunorsm; av\muxm;Eiyg on/

- ouaocvurwav\muxm;ou,wi ?
- urP? tztpn;trnjzi av\muxm;yg u w&m;0irwywixm;aomurP ? tztpn;\ w&m;0iu,pm;v, (Any Authorized Representative) ?
- MOSS CA \ w&m;0i u,pm;v,rsm; ?
- RA \ w&m;0i u,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 tc\utvursm;jzi jznpuay;&rn/ ouaocvurwav\muxm;otm;v;on ouaocvurw im;&r;o;po oabmwnc\u (Subscriber Agreement) wi yg0iaom tc\ursm; ? tmrcc\ursm;u oabmwnr&&rn/ ouaocvurwav\muxm;or Key Pair (Public Key Ei Private Key) u rrbmom jy\vyyg u

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

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

vtyyg u ouaocvurwav\muxm;ou,pm; MOSS CA (o) RA r Key Pair Generate jy\vyay;jci;u aqmi&uyg on/

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 tc\utvursm;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/

MOSS CA (o) RA on atmuazmjyygtc\ursm; jzpym;v\i ouaocvurw xway;jci;u 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;pmrsm;u owrwtc\etwi; ta&;,aqmi&ujci;? ta\umi;jye\um;jci; r&cv\i ?
- owrwxm;aom aia\u;uay;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 \ *Poum xcueion[,qv\i ?

4.2.3 ouaocvurwav\muxm;jci;u vucaqmi&uay;on\umjric\e

(Time to Process Certificate Applications)

ouaocvurwav\muvmEitw vtyaom y;wtaxmutxm;rsm; jynppm jznpu wijyjy;ontc\erpí MOSS CA (o) RA on ouaocvurwxway;&e aqmi&uygon/ ouaocvurwtm; tvyvy&u (7)&utwi; xway;ygon/ CA r ouaocvurw xw,Eia\umi;u av\muxm;otm; e-mail (o) pmjzi (o) ze;jzi ta\umi;lum;ygon/ ouaocvurw av\muxm;jci;on jii;y,jci; ? y,zujci;rc&ontc\etx 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 tcsutvursm;u to;jy|í ouaocvurw xway;ygon/ ouaocvurwxw|y;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 ouaocvurwu RA x av|muxm;ou,wi vma&muxw,&rn/ ouaocvurwtrs|;tpm; (Class 1) twu WebSite r download vyíaomvn;aumi; ? vu,wirvma&muEiygu u,pm;xw,Ei&e vn;aumi; pp0xm;ygon/ av|muxm;oon Public Key wpcxuyí ouaocvurw xway;&eav|muxm;ygu xway;onouaocvurwta&twut& usoiaiu ay;aqmi &rnjzpygon/ MOSS CA on vurwa&;x;jci;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 MOSS 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;jy|í talumi;lum;ay;ygon/

4.4 ouaocvurwuvucjci; (Certificate Acceptance)

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

ouaocvurwtm; download jy|vyí &,cv|i (o) ouaocvurwyg tcsutvu rsm;Ei ouaocvurwon rm;,i;alumi; MOSS CA (o) RA xxway;on&urpí (15) &utwi; ueuupmay;yjci;r&cv|i ouaocvurwtm; vucon[owrwygon/

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

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

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

4.5.1 Subscriber \ Private Key Ei ouaocvurwto;jyr

(Private Key and Certificate Usage)

ouaocvurwu to;jyoon im;&r;o;porm;\ oabmwncu (Subscriber Agreement) Ei CP ? þ CPS wwiyg0ion owrwcurm;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 uvyaqmicirjycvji ouaocvurwu vurwa&;x;&etwu to;jyjci; rjyvy &yg/)

ouaocvurwo;porm;on rrw\ Private Key rm;utcir&aomor to;rjyEi&e umu, aqmi&uxm;&rn/ ouaocvurwouwr;ueq;jy; aemuyi;Ei y,zuly; aemuyi; wi xouaocvurwu quvuto;rjy&yg/

4.5.2 Relying Party r Public Key Ei ouaocvurwto;jyrrm;

(Relying Party Public Key and Certificate Usage)

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

ouaocvurwwpcay:wi ,luno;pron tajctaetrs;rs;ay:rwnítalumi; tus;oiavsmr &?r& u Relying Party rsm; u,wip0;pm;? q;jzwívuc&rn/ tu,í tajctaewpconaemuxytmrccurm;&,oion[,qygu Relying Party on xo ,lun o;pjci;jyvy&etwu vtyaomtmrccurm;u xyr&,&rn jzpygon/

xuoaom ,luno;prrm; rjyvyr Relying Party rm;on atmuygtcuwu vwvypm o;oyjci; (assess) jyvy&rn/

- Certificate wiazmjyxm;on to;jyrv &n&,cut& ouaocvurwtm; to;jyjci;rm oiavsmr &?r&?
- þ CPS r wm;jrp ? ueowxm;jci;r&aomoiawmon&n&,cuwpctwu tre wu, to;jyjci;[w?r[w?
- ouaocvurwEi ,i;ouaocvurwu xway;caomo (Root CA, CA) rsm;\ ouaocvurw tajctaersm; (Status) uppaq;&rn/ ouaocvurw Chain wiyg0iaomouaocvurwwpccon y,zujci;cxm;&aomouaocvurw jzpygu

Relying Party on xouaocvurwu ,lun&e oi ? roiEi y,zsuc&rrm us;alumi; qavsmr&?r&u to;rjyr ppr;ppaq;&e wm0e&ygon/

MOSS CA Ei RA rsm;on ouaocvurw to;jyjci;\ oiavsmr&?r&u ppaq;&e wm0er&y/ ouaocvurwo;pron oiavsmon[,qvli Relying Party rsm;on oiavsm on Software Ei (o) Hardware uto;jyí 'p*spw,vurw (Digital Signature) reuealumi; ppaq;r (Digital Signature Verification) u jylvyjci;aomvn;aumi; ? tjcm;aom Cryptographic Operation uto;jyíaomvn;aumi; ouaocvurw\ reueruppaq;&rn/ þuo ppaq; aqmi&urrsm;Ei ouaocvurwtay:wi ,luno;prwon qupyygon/ xuo jylvy ppaq;aqmi&ujci;wi Certificate Chain wpcowrwjci;Ei ,i; Chain wiyg0iaom ouaoc vurwtm;v;\ Digital Signature rsm; reuealumi; ppaq;jci;wvn;yg0iygon/

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

Certificate Renewal on vu& Key Pair tm;to;jyjy; ouaocvurw ouwr;w; avmuxm;jci;rs;jzpygon/ ouwr;w;jci;u ouaocvurw ouwr;rueq;r (1) v lulwi avmuxm;&rn/ Key Pair ouwr; (2) Epjynjy;ygu Key Pair topwppo;í ouaoc vurwtopjylvy&e MOSS CA x avmuxm;Eiygon/

4.6.1 ouaocvurw ouwr;w;jci;tajctae (Circumstances for Certificate Renewal)

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

4.6.2 ouaocvurw ouwr;w;avmuxm;ci&o (Who Can Request Renewal?)

ouaocvurwavmuxm;ou,wi (o) tztpn;jzpygu tztpn;\ouaoc vurwavmuxm;jci;uprsm; aqmi&u&etwu w&m;0ipmjziwm0eay;tyxm;on u,pm; v,romvli ouaocvurwouwr;w;jylvy&e awmi;qEiygon/

4.6.3 ouaocvurw ouwr;w;jci;aqmi&ur

(Processing Certificate Renewal Request)

ouaocvurwouwr;w;jylvy&mwi rvavmuxm;co trewu,jzpalumi; aocsmap&e MOSS CA (o) RA rjyeíppaq;ygon/ Class 1 ouaocvurwtwu Challenge Phrase (or[w tvm;w Phrase) wpcu to;jyíaomvn;aumi; ? Private Key yiqijci;u

ouaojyíaomvn;aumi; ? Renewal Request uvucygon/ im;&r;o;porm;on ouaoc vurwavmuxm;p0u jznpucaom Information rm;Eitw Challenge Phrase (or[w tvm;w pum;p) wpccua&;c,ay;y&rn/ im;&r;o;poon Certificate topwpc jyevn jyvyontcg ¤i;\ Challenge Phrase tygt0i avmuxm;p0ujznoi;caom tcutvurm; ajymi;vrr&cvi ouwr;w;ouaocvurwu xway;ygrn/ ouwr;w;ouaocvurw avmuxm;vmontcgwi;wi rvouaocvurw avmuxm;p0u MOSS CA (o) RA r ppaq;on en;vr;rm;Ei þ CPS wi owrwxm;aom ppaq;&rn tcurm;Eitn avmuxm;o\ Identity u jyevnppaq;twnjyrn jzpygon/

4.6.4 ouaocvurwtop xw,Eialumi; im;&r;o;pootalumi;lum;jci;

(Notification of New Certificate Issuance to Subscriber)

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

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

(Publication of the Renewal Certification by MOSS CA)

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

4.7 Key Pair toputo;jyíouaocvurwouwr;w;jci; (Certificate Re-Key)

Certificate Re-Key on Public Key topwpcu to;jyí ouaocvurwtopwpc xway;jci;jzpygon/

4.7.1 Key Pair topu to;jyí ouaocvurw ouwr;w;&e tajctaerm;

(Circumstances for Certificate Re-Key)

Certificate Re-Key on ouaocvurwwpc\ vu&to;jyaeaom Private Key vjcl pwc&ru oo,&aomtcg (o) vu&o;paeaom Key rm;\ouwr; (2) Ep jynaomtcgwi jyvyEiygon/ xuo ouwr;w;jci;u ouaocvurw ouwr;rueq;r (1) v lulwi avmuxm;&rn/

4.7.2 ouaocvurwtopjyevnjyvy&eawmi;qci&orm;

(Who May Request Certificate of a New Public Key)

ouaocvurw ouwr;w;jci;twu Class 2 Ei Class 3 ouaocvurwrm;jzpygu im;&r;o;pou,wiromvi (or[w) tztpn;\ ouaocvurwtwu vtyxm;aom w&m;0iu,pm;v,romvi ouaocvurwtopjyevnjyvy&eawmi;qEiygon/

4.7.3 Key toptoíjyí ouaocvurwouwr;w;&eawmi;qjci;u aqmi&ujci;

(Processing Certificate Re-Keying Requests)

Key toptoíjyí ouaocvurwouwr;w;&eavmuxm;oon rvouaoc vurw avmuxm;ou,wi (o) w&m;0iu,pm;v, trewu,jzpalumi; ppaq;jci; Ei Authentication jzp&etwu owrwxm;aomvtycsurm;Ei avmnpm jyevnppaq;jci;wu MOSS CA (o) RA on vyx;vyen;rm;twi; (Challenge Phrase (or[w tvm;w Phrase) wpcu toíjyíaomvn;aumi;? Private Key yiqiru ouaojyíaomvn;aumi;) aocmpm ppaq;ygon/ xo ppaq;atmijrijy;aom avmuxm;orm;tm; ouaocvurwrm;xway;jy; im;&r;o;porm;xo ouwr;w;ouaocvurwxw,Eialumi; talumi;lum;pmay;yrn jzpyg on/

4.7.4 Key toptoíyí ouwr;w;xm;aom ouaocvurwu xw,Eialumi; im;&r; o;pootalumi;lum;jci; (Notification of New Certificate Issuance to Subscriber)

Key toptoíyí ouwr;w;xm;aom ouaocvurwtopu xw,Eialumi; im;&r;o;poo talumi;lum;jci;u ty' (4.3.2) twi;aqmi&uygon/

4.7.5 Key toptoíjyí ouwr;w;xm;aom ouaocvurwtm; xwjyealunmay;jci;

(Publication of the Re-Keyed Certificate by the CA)

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

4.8 ouaocvurwjyfjyiajymi;vjci; (Certificate Modification)

4.8.1 ouaocvurwjyfjyiajymi;vrtajctaersm;

(Circumstances for Certificate Modification)

ouaocvurwjyfjyiajymi;vjci; (Modification) on im;&r;o;po\ Public Key r v í vu& ouaocvurwwpcwiyg0iaom tcsutvursm;ajymi;vralumi ouaocvurw topwpcxway;&etwu avmuxm;jci;u &nne;yg on/ ouaocvurwjyfjyi ajymi;vjci; (Modification) on ty' (4.1) wiazmjyxm;aom ouaocvurwavmuxm;jci;Ei wnon[p0;pm;yg on/

4.8.2 ouaocvurwjyfjyiajymi;v&eawmi;qci&o

(Who May Request Certificate Modification)

ty' (4.1.1) twi;aqmi&uyg on/

4.8.3 ouaocvurw jyfjyiajymi;vay;&e awmi;qrrm;u aqmi&ujci;

(Processing Certificate Modification Requests)

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

4.8.4 ouaocvurwtopxwjy;alumi; im;&r;o;porsm;o talumi;lum;jci;

(Notification of New Certificate Issuance to Subscriber)

MOSS CA (o) RA on ouaocvurwtopxwjy;yg u avmuxm;oxo t;ar;(v) (o) pm (o) tjcm;aomen;vr;rsm;u to;jyfí talumi;lum;rnjzpyg on/

4.8.5 jyfjyiajymi;vjy;aom ouaocvurwuvucjci;

(Conduct Constituting Acceptance of Modified Certificate)

ty' (4.4.1) twi;aqmi&uyg on/

4.8.6 jyfjyiajymi;vjy;aom ouaocvurwuxwjyeay;jci;

(Publication of the Modified Certificate by the CA)

ty' (4.4.2) twi;aqmi&uyg on/

4.9 ouaocvurwy,zujci;Ei,m,qi;ijci; (Certificate Revocation and Suspension)

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

(Circumstances for Revocation and Suspension)

MOSS CA (o) Subscriber u,wir y,zu&e awmi;qrom ouaocvurwu y,zuí CRL wi xwjyealunmay;ygon/ im;&r;o;pory,zujci;jyvyvyguw&m;0ipmjzi a&;om;avmuxm;&rn/ ouaocvurwuy,zu&etwu vavmuaomtaxmutxm;? talumi;jycsu&gu MOSS CA on ouaocvurwu y,zuEiygon/ atmuyg tajc taersm;jzpay:cvi MOSS CA on im;&r;o;porsm;\ ouaocvurwrsm;u y,zuEiygon/

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

(2) im;&r;o;poonvuem&rnpn;ur;rsm; (Subscriber's Obligation, Representation) (o) Subscriber Agreement yg tmrccsu (Warrenty) rsm;u c;azmuon[MOSS CA r,luny; talumi;jycsursm;? ouaorsm;&cvi ?

(3) im;&r;o;poEi cyqxm;aom oabmwncsupmcsyrsm; &yp/jy;q;om;vi ?

(4) Class 3 Organization Certificate rsm;twu tzjtpn; (Affiliation) zsuor;vi (o) r&awmvi ?

(5) MOSS CA r ouaocvurwon Subject Field wiyg0ion trnr[wo wp0;tm; xway;xm;jci;? ¤i;y*vcijycsur&&y ouaocvurwu xway;on[,qly; talumi;jycsu&cvi ?

(6) ouaocvurwavmuxm;&mwi jznoi;xm;ontcsursm; rm;,i;aevi ?

(7) ouaocvurwxway;jci;rjyr y;wwijy&rntcsursm; jynpatmiaqmi&u jci; r&cvi ?

(8) im;&r;o;po ? tzjtpn;trn ? ouaocvurwwiyg0iaom Common Name (CN) ajymi;vcvi ?

(9) ouaocvurwygtcsutvursm;reuerr&alumi;Eiajymi;vom;alumi; ppaq; azmxwaw&cvi ?

(10) ouaocvurwu quvuo;pygu Root CA/ MOSS CA Ei tjcm;o;porsm;tm; jyóemjzpEicvi ?

(11) ouaocvurwu w&m;r0ixw,xm;alumi;aw&&vi ?

ouaocvurw quvuo;pralumi jyóemjzpjci;& ? r& q;jzw&mwi atmuyg tcsursm;u xnoi;p0;pm;ygon/

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

(2) wiwe;rjyvyoon rnorn0gzponu 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;iyrrsm;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&e awmi;qci&o (Who can Request Revocation)

im;&r;o;pou,wi (Individual) (o) tzltpn; ouaocvurwjzpygu wm0eay;ty xm;aom w&m;0iu,pm;v,rom y,zsu&eawmi;qEion/ im;&r;o;po\avmuvmu twnjylay;o (approve vyo) MOSS CA Ei RA u,wirvn; ouaocvurwu y,zsuEion (o) y,zsu&e awmi;qEion/

4.9.3 ouaocvurwy,zsu&e awmi;qrvyen;

(Procedure for Revocation Request)

ouaocvurwy,zsu&e o;porsm;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,zsujci;avmuvmypu MOSS CA \ Website jzpon http://www.moss.com.mm wi download &,Eiygon/

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

ouaocvurwu y,zsu&e awmi;qrrsm;twu qi;icserxm;yg/

4.9.5 ouaocvurwy,zsu&eawmi;qjci;twu MOSS CA raqmi&u&e lumjricse (Time within which MOSS CA must process the Revocation Request)

MOSS CA on Revocation Request u ouqi&mwm0ec\ cijycsu&vli aEmiaE; luelumrr&apy (24) em&twi; owrwxm;aom tqirsm;twi; vyaqmiom;ygrn/

4.9.6 Relying Parties rouaocvurwy,zsujci;u ppaq;&evtycsursm;

(Revocation Checking Requirements for Relying Parties)

Relying Parties rsm;on rrto;iyrn ouaocvurwrsm;\ pwcs&rtajctae (Status) u ppaq;&rn/ ouaocvurw\pwcs&rtajctae (Certificate Status) u ppaq;&mwi-

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

2/ MOSS CA \ Web-based Repository (o) OCSP (&yu) to;jyí ppaq;jci;?

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

Relying Parties rm;on MOSS CA \ Repository Ei CRL rm;? National Repository? OCSP Responder (&yu) rm;uto;jyí ouaocvurw\ pwc&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 wpywwpur xwjyeay;rn/ CRL x& ouaocvurwwpc ouwr;ueq;jci; (Expire) jzpvli ¤i;ouaocvurwu CRL r xwy,ay;rnjzpygon/ MOSS CA on ouaocvurwim;&r;opo rm;\ ouaocvurwy,zupm&i;u y,zu&eawmi;qjci;tm; cijyontcgwi; xwjyeay;rn/

4.9.8 ouaocvurwuy,zujci; trm;q;lumjricte (Maximum Latency for CRLs)

MOSS CA r ouaocvurwwpcu y,zucontcg y,zujy;vlijy;ci;4i;\ Repository wi xwjyeay;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 (&&Eivli) 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;jyvy&e vtycurm; (On-line Revocation Checking Requirements)

ouaocvurwu ,lunpwcívucto;jyorm; (Relying Party) rm;on rrvuc to;jyrn ouaocvurw\ ,lunpwc&rtajctae (Status) uppaq;&rn/ Relying Party on ouaocvurw\ ,lunpwc&rtajctaeu aemuq;xwjyecon ouqion ARL/ CRL uto;jyíppaq;jci; rjyvyygu MOSS CA \ Repository Ei National Repository &

ouaocvurw tajctae (o) to;jy\Eion OCSP Responder (&yu) wu to;jy\í ppaq;&rn/

4.9.11 Key c\;azmuc&jci;Eiouqiaom tx;aqmi&uc\urm;

(Special Requirements Regarding Key Compromise)

MOSS CA on rr\ Private Key c\;azmuc& (Compromise) on[aw&v\i (o) xo\zpon[ta\umi;jyc\u ouaocivr&v\i ¤i;\ Potential Relying Party rm;tm; ta\umi;\um;jci;u wwEior\jy\vyay;rn/

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

jyXme;xm;jci; r&yg/

4.9.13 ouaocvurwu,m,qi;i&e awmi;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\&rtajctae 0eaqmirrm; (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 (&yu) wwi 0ia&mu\un&\Eiygon/

4.10.2 ouaocvurwEiqiaom0eaqmir &&Eir (Service Availability)

ouaocvurwpwc\&rtajctae 0eaqmirrm; (Certificate Status Service) u (24)em& (7)&uywv; &&Ei&e aqmi&uxm;ygon/

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

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

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

2/ ouwr;rueq;r rr\ ouaocvurwu y,zuly; 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. taxmu tyrsm;? prcecjci;Ei vyie;aqmi&ujci;qi&m xe;cslyrrsm;

(Facility, Management and Operational Control)

5.1 MOSS CA vyie;\ &yyi;qi&mxe;csly? 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 vlcr&ap&e? rouqiorsm;r usl;ausm0ia&mujci;? to;jyjci;r&ap&e? vw0uowi;tcsutvursm;Ei peprsm;u rouqiorsm;rlun&jci; rlyvyEi&e &yyi;qi&mumu,on yw0e;usi** (Physically Protected Environment) **u xm;&to;lyí aqmi&uygon/** MOSS CA **on vjcr&ap&etwu tce;rsm; wnaqmujci;u tvuxa&mepquo,aqmi&ua&;0ya'?,i;Eiqupyon en;0ya'rsm;? trealumjimpmrsm;? vr;necursm;twi;aqmi&uxm;ygon/**

5.1.2 vyie;aqmi&u&m ae&mo0ia&mujci; (Physical Access)

MOSS CA **on 4i;\pepvlcla&;twu tqi** (Tier) **rsm; cjcm;ly; vlcla&;ppaq;xm;yg on/ twi;yi;& vjcrtqiyjrionae&m** (Higher Tier) **rsm;u 0ia&muto;jy&e tjyiyi;& vjcrtqiyeronae&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; aomae&mrsm;o wu&uwm0e&orví tjcm;orsm;tm; 0ia&muciryly/**

Cryptographic Material **rsm; xway;** (Create) **on? or;qn;** (Store) **xm;on ae&mrsm;o 0ia&mujci;? pprealumi;taxmu txm;pppjci;** (Authentication) **u** Biometrics **en;ynmo;í** (2

Factor Authentication) jzixe;cs yxm;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*|vrsm; 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 vlca&;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&url (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;tyce ? av0iavxu ? avat;ay;pep ? pxi;r (Humidity) wu Control jylvyxm;ly; ,i; System wivn; Primary Ei Backup peprsm;jzi cjcm;pp0aqmi&u xm;&ygon/

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

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

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

r;ab;tE&m,rumu,Ei&e vtyonu&,mrsm;wyqijci;Ei umu,jir;owrn tp tp0rsm; 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;&;rr&ap&e umu,xm;&ygon/

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

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

5.1.8 vlcpwcs&on tjcm;wpae&mwi Backup jyivyor;qn;jci; (Off-Site Backup)

MOSS CA on Audit Log Data rsm;Ei ta&;u;onowi;tcsutvu (Sensitive Information) rsm;yg0ion ta&;u;onpep Data rsm;u vlcpwcs&on tjcm;wpae&mwi Backup jyivyí ae&mcjcm;ly; or;qn;xm;ygon/

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

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

MOSS CA on ,lunpwcs&onae&m (Trusted Position) wiwm0exr;aqmirn ,lun pwcs&aomy*lvrsm; (Trusted Person) [owrw&mwi atmuazmjyyg vyie;rsm;u aqmi&uaeon 0exr;rsm;tm;v; ? pmcsyEivyie;vyuio (Contractor) rsm;Ei tluay;/ twiyicy*lv (Consultant) rsm; ? tvuxa&mepquo,aqmi&ua&;A[tzEi lu;luyrtzr trepmjzi w&m;0iwm0eay;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 ?
- ouaocvurwtopavlmuxm;jci; ? ouwr;w;avlmuxm;jci; ? y,zsu&e avlmuxm;jci; (o) Enrollment Information rsm;u vucjci; ? jii;y,jci;rsm;u aqmi&uorsm; ?
- ouaocvurwrsm;u xway;jci; ? qi;ijci; ? y,zsujci;aqmi&uorsm; ? ouaocvurw rwwr;rsm; (Repository/ LDAP /OCSP (&ygu) \ ueowxm;aom ae&mrsm;o 0ia&mulyjyiajymi;vjci; ? xnoi;jci; ? zsujci; aqmi&u&e tci&o tm;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; ?
- ouqionti*sie,mrsm; ?
- Infrastructure \vlcpwc&rtwu praqmi&uo txutqit&m&rsm; yg0iygon/

MOSS CAr ,lunpwc&aomy*lv (Trusted Person) rsm;on owrwxm;aom t&n tcsi;rsm;? owrwcsursm; (Screening Requirement) Ei jynpuunr&ygon/

5.2.2 vyie;wpccsi;ptwuv tyrn0exr;ta&twu

(Number of Persons Required Per Task)

MOSS CA on wi;usyaomvyx;vyen; (Control Procedure) rsm;owrwxm;&ly; xtwi;aqmi&ur&ap&e wm0e (Duty) rsm; o;jcm;ca0csxm;jci; ? ta&;su;on vyie;rsm;wi 0exr;rsm; wp0;xuru wm0e,aqmi&uromjy;ajrmu&e ca0aqmi&uapjci;jzi xe;clyr (Control) jylvyxm;ygon/

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

Internal Control Procedure rsm;taejzi vlcrtwuta&;su;on tcsutvursm; ? puypn;u&,mrsm;u uiw,aqmi&u&mwi (Physical Access or Logical Access tygt0i) ten;q;v (2) a,muxm;&ly; aqmi&uromvyie;ly;ajrmuatmi aqmi&uEirn tptp0rsm; xm;&aqmi&uygon/ ypn;rsm;uuiw,to;jylí vyie;aqmi&u&mwi wp0;wn;Ei vyie; tprtq;o aqmi&uEijci;r&ap&e Control rsm;uca0xm;ygon/

ouaocvurw avlmuvmwpapmia&muvmonrpí ppaq;jci; ? ouaocvurw xway;jci; ? ouwr;w;jci; ? y,zsujci; ? aemuq;wizsuq;ypjci;pon Life-Cycle wpcv; u ,lunpwc&on 0exr;rsm;xm;&ly;aqmi&uygon/ Physical Access Ei Logical Access u ta&;su;onae&mrsm;wi o;jcm;vrsm;uo;í cjcm;xm;ygon/

5.2.3 0exr;wp0;cs;p\vyie;wm0ers;Eippaq;ru@

(Identification and Authentication for each Role)

MOSS CA **\ ,lunpwc&aom 0exr;tjzpcexm;rn vjcla&;tqijrit&m&rs;** (Top Level Security Related) **tm;v;uvawppaq;jci;?rwywiEi tjcm;vtyaom taxmutxm;rs; to;jy(íppaq;jci;rs; aocspm jy(vy(y;rom0exr;tjzpcexm;ygon/ vtyygu** Background Check **rs;jy(vy(y;rcexm;jci;jy(vyygon/ 0exr;tjzpcexm;(y;aemu ouqi&m txu vsu;\oabmwncsu&&jy;rom pm&upmwr;rs;?uey(wmEi qupyypn;rs;?** Software **rs;u uiw,o;p** (Access) **ciay;jci;?tvuxa&mep** Data **rs;u lun&ci?vyie;vyaqmici ay;ygon/**

5.2.4 vyie;wm0ers;ca0r (Roles Requiring Separation of Duties)

vyie;wm0ers;ca0owrwjci;wi atmuygwyg0iygon/

- **ouaocvurwav(muxm;jci;wi yg0iaom tcsutvurs;u ppaq;jci;?**
- **ouaocvurwav(muxm;jci;?y,zsujci;?ouwr;w;jy(vyjci;?tcsu tvurs;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\tcsutvurs;?awmi;qjci;rs;u uiw,ajz&i;jci;?**

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

5.3.1 0exr;rs;\t&ntcsi;vyie;tawtlu(Ei Clearance vtycsurs;

(Qualifications, Experience, and Clearance Requirements)

,lunpwcs&aom0exr;tjzp av(muxm;orsm;on ¤i;w\aemualumi;&mZ0i (Background) **?ynmt&ntcsi;?rrwm0e,aqmi&urnvyie;Eiywouaom vyie; tawtlu(wu jynppm wijyav(muxm;&rn/ vtyygu ,civyie;rs;r&i;vi;r** (Clearance) **u,&rn/** Trusted Position **wi&aeon 0exr;rs;tm; aemualumi;&mZ0ippaq;jci;** (Background Check) **u ten;q;(5) Ep wp\ur jyevnjy(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;ycsr\rsm; (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;jyevnycjci;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/ usl;veontlura& Ei azmuzsurtwi;twmay:wi 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;jy[vyjci;tptrrsm; (Audit Logging Procedures)

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

MOSS CA on Manual Log (o) Automatic Log rsm;xm;&ly; atmuazmjyyg tjzptysursm; twu pm&i;pp rwwr;xm;&ygon/ rwwr;xm;&aom tjzptysuwi;wi ae&u? tcteEi þ tjzptysuu jzpay:apon ta[umi;&i;wyg0iygon/

1. vyie;aqmi&ujci;qi&m tjzptysursm; -
   - CA Key rsm;jy[vyjci; ?
   - CA pepEi Application rsm; Start-Up Ei Shutdown jy[vyjci; ?
   - 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;
   - ouaocvurwav[muxm;jci; ? ouwr;w;jci; ? y,zsujci;Ei Re-Key/Renew jy[vyjci;rsm; ?
   - ouaocvurwrsm; ? CRL rsm; ? Generate jy[vyjci; ? 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;o ci[jycsur&b 0ia&mu&elu[;yr;rrsm; ?
   - v[W0uzirsm; ? rwwr;rsm;zwjci; (Read Access) ? a&;jci; (Write Access) ? zsuq;jci;rsm; (Deletion) ?
5. ouaocvurwEi ouaocvurw rwwr;wu (Repository) ay:wi zwjci; ? a&;jci;w aqmi&ur&&rrsm;

6. ouaocvurwjy[vyjci;qi&mr0g'ajymi;vrrsm; (0yrm-Validity Period ajymi;vjci;)
7. taxax

- vjcla&;qi&mrwwr;rsm;Ei xrwwr;rsm; (SecurityProfile) wi ajymi;vjy[jyixm;rrsm; ?
- pep,m,cs[,i;;jci; (Crash) rsm;? Hardware Failures rsm;Ei tjcm;aom yrer[won up&y (Anomalies) rsm; ?
- Firewall Ei Router Activity rsm; ?
- 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?tcsEi talumi;t&m?
- rwwr;pmtywi a&;oi;&ygu rwwr;wio\trn?

8. A[tz?lu;luyrtzEi Root CA wr rwwr;tjzpor;qn;&evtyon[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; jy[vy&mwi log rwwr;rsm;wi jy[jyixm;rrsm; &?r& ppaq;jci;Ei Audit log a&;om;cursm; tm;v;u jyevnppaq;jci;? yrer[waom uprsm;? oway;csursm; (alerts) uppr; ppaq;jci;rsm; yg0iygon/

ta&;ygon vlcla&;qi&mtjzptysursm; ? up&yrsm;twu wpywv[i ten;q; wplur ppaq;rrsm;jy[vyygon/¤i;tjyi MOSS CA on¤i;\ Audit Log File rsm;r oo,jzp Eion or&;usr[waom ? yrer[waom tjzptysursm;u tlrwr; ppaq;ly; oway;csu xwjyejci;? ppr;ppaq;jci;rsm; jy[vyygon/ Audit log review jy[vyxm;onrsm;uvn; rwwr; xm;&ygon/ MOSS CA \ vyie;qi&mrwwr;rsm;u Root CA o (6) vv[iwplur wijyyg on/

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 vlcpwc;&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&urn tptp0 (Audit Log Backup Procedures)

Audit Log rsm;u aep0vyie;vyaqmior| Backup jylvyly; wpywwp|urtjynt0 (Full Backup) jylvyygon/

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

tvtavsmu Audit Data rsm;xwjci; ? rwwr;xm;jci;wlu Application / Network Ei Operating System Level twi; aqmi&uygon/ 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;rjylvy&rn/ pep wpcv;\ jzpEiaomysup;q;&;rrsm;wi;wmppaq;jci;u Log Data rsm;wi rwnppaq;ly; aep0 ? vp0Ei Epp0 jylvyygon/

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

(c) Physical Facilities rsm; ?

(*) Network peprsm; ?

(C) pm&i;ppjci;qi&m tjzp tysursm; (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;pptc;utvu (Audit Data) tm;v; ?

- ouaocvurwxway;jci;Ei ouqion y;wyg taxmutxm; ? pm&u pmwr; (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 \ouaocvurwxway;jci;qi&mrwwr;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&onorsm;uom lun&cijyí rouqio rsm;r lun&jci; ? jyiqijci; ? zsuq;jci; ? rwwr;rsm;wi jyjyijci;rsm;rjyvyEi&e umu, xm;&ygon/ þ CPS 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;&rntptp0 (Archive Backup Procedure)

ouaocvurwrsm;\ tcsutvursm;u aep0 Incremental Backup, tygwp0 Full backup jyvyygon/

owi;tcsutvursm;u rwwr;a[mi;tjzp xm;&&mwi trsm;pu tvuxa&mep Record ypjzixm;&í vtyygu pm&upmwr;ypjzi or;qn;jy; xrwwr;rsm;u vjcon tjcm; wpae&mwi rwu;í xe;or;xm;&rnjzpjy; ysup;rr&ap&evn; twwEiq; pepwuspp0 or;qn;xm;&ygon/

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

(Requirements for Time-Stamping of Records)

ouaocvurwrsm; ? CRL rsm; ? tjcm;aom y,zsujci;qi&m rwwr; Revocation Database) rsm;wi tcseEiae&uu rwom;xm;ygon/ CA Computer System \ Time Clock u

ppr;ppaq;rrsm;wi u;usm;to;jyEi&etwu a'opawmc:eEi uunr&ap&e aqmi&uxm;& ygon/ xuo tc:eqi&mrwom;rrsm;on Cryptographic ay:wi tajcc&ervyg/

5.5.6 rwwr;tc:utvursm;ppn;r (Archive Collection System (Internal or External))

MOSS CA \ rwwr;a[mi; paqmi;on pep (Archive Collection System) xm;&ygon/ MOSS CA \ ,lunpwc:&aom0exr;rsm;rom rwwr;tc:utvursm;u vyuiaqmi&uci&yg on/

5.5.7 rwwr;rsm;&&r Ei ppaq;r vyie;p0rsm;

(Procedures to Obtain and Verify Archive Information)

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

5.6 CA Key Pair topjylvyjci; (Key Changeover)

MOSS CA \ owrwxm;aom Key ouwr; (Maximum Life Time) u ausmveygu CA Key Pair rsm;u vyie;wi quvuto;rjyly/ CA Key Pair ouwr; rueq;r ten;q; (12) v lulwií ouwr;w;jci; jylvy&rn/ CA Key Pair topwpp vtyontcgwi;xwygon/ (0yrm- CA Key pair ta[mi;u tpm;x;&e ? vu& Key Pair \ lznzutjzp to;jy&e ? 0eaqmir toprsm;ay;&e)

CA Key Pair ta[mi;r topo u;ajymi;&mwi v,uacsmarlpm u;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 &ypvuon 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;r jyevnxaxmijci;

(Compromise and Disaster Recovery)

5.7.1 rawmwqrEi csi;azmuc&rrsm;u uiw,ajz&i;rnvyx;vyen;rsm;

(Incident and Compromise Handling Procedures)

MOSS CA \ tcsutvursm;?(ouaocvurwavjmuxm;jci;qi&m tcsutvursm;? pm&i;pp Data rsm;? xway;xm;aom Certificate rsm;\ database records rsm;) \ Backup uvjcon tjcm;wpae&mwi xe;or;xm;&y; rawmwqrEi csi;azmuc&rrsm;jzpym;ygu tqioi&&Ei&e aqmi&uxm;ygon/ MOSS CA on rawmwqrEi csi;azmuc&rrsm;u uiw,ajz&i;rn tptrrsm;aqmi&uxm;&ygon/ ,i;tptrwi ten;q;atmuazmjyygtcsursm;yg0iygon/

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

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

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

5.7.2 ueysiwmEi qupyypn;rsm;?aqm0vEi tcsutvursm;ysup;q;&;ru aqmi&ujci;

(Computing Resources, Software and/ or Data are Corrupted)

ueysiwmEi qupyypn;(Computing Resources) rsm;?Software rsm;?Data rsm;pon wwi ysup;q;&;r (Corruption) rsm;jzpym;ygu iu;iuyrisz Ei Root CA otp&icpmwijyiy;CA \ vica&;Eirawmrqrrsm;u uiw,ajz&i;rn vyx;vyen;rsm;(Incident Handling Procedure) twi;aqmi&uom;rn jzpygon/ xvyx;vyen;rsm;wi ueysiwmEi qupyypn;(Computing Resources) rsm;?Software rsm;?Data rsm;ponwu oiavsmonae&moa&iajymi;jci;?rawmwqru ppr;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 csi;azmuc&jci;twu aqmi&urvyie;p0rsm;

(Entity Private Key Compromise Procedures)

MOSS CA \ Private Key (o) Infrastructure rsm;csi;azmuc&jci;(Compromise) jzpon[oo,jzpygu (o) o&ygu (o) xo jzpysuon[taxmutxm;civygu MOSS CA r tzizIy;tajctaeuavvmqe;ppjci;?iu;iuyrtzEi Root CA otp&icpmwijyjci;?Action Plan a&;qjci;?Action Plan twi;taumitxnazmjci;rsm;u tqiqivyaqmiom;rn jzpygon/ tu,í MOSS CA \ ouaocvurwuy,zu&evtyygu -

- xo y,zualumi;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,ua&mujy;aemu vyie;rsm; quvuvnywEirpr;&n

(Business Continuity Capabilities After a Disaster)

MOSS CA on ab;tE&m,rsm;alumi yup;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/ wuEiorlyuq;q;&;r en;ap&e aqmi&uxm;ygon/ þ Plan u Disaster jzpym;ygu vyie;aqmi&uEiap&e yreppaq;jci; ? cteuujci; ? ajymi;vjyfjyijci;rsm; jylvyygon/ t"u CA vyie;rsm;jzpon -

- ouaocvurwxway;jci; ?
- ouaocvurwy,zujci; ?
- ouaocvurwy,zujci;qi&m tcutvursm;xwjyejci;rsm;u tcewtwi; jyevn aqmi&uEi&e pp0xm;&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;rsm;Ei Software rsm;uvn; t&Ei Backup rsm;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;porsm; ? Relying Party rsm;tm;xcuepemr ten;q;jzpaprn Termination Plan u a&;qxm;ygon/ Termination Plan wiatmuygtcursm; twi; praqmi&uygon/

- tjcm; CA rsm; ? im;&r;o;porsm;Ei ouqiotm;v;tm; lulwitalumi;lum;jci; jylvyygrn/ xtcterpí MOSS CA on rnon ouaocvurwxway;jci;ur rjylvyyg/

- CA vyie;rsm;&ypjci;jy\vyawmrntalumi; Website Ei owi;pmrsm;wivtrsm;oom ap&e\ulwixwjyealujimay;jci;?
- MOSS CA \ rwwr;a[mi; (Archive) rsm;? rwwr;rsm;? Database rwwr;rsm;Ei pm&u pmwr;rsm;u &yponaerpí þ CPS wi owrwxm;onumvtx xe;or;xm;&jci;?
- MOSS CA \ Repository Ei CRL u &ypjy;onaerpí (12) vtx trsm;jyno 0ia&mu \un&Eiatmi pp0xm;&jci;?
- Customer Support 0eaqmir (Service) rsm;uquvu o;pEi&epp0jci;?
- CRL rsm;xwjyejci;? ouaocvurw,\unpwc\&rtajctaeppaq;on 0eaqmir (Certificate Status Checking Service) rsm; quvuaqmi&uEi&e prjci;?
- ouwr;rueq;ao;aom ouaocvurwtm;v;u \ulwitalumi;lum;umv jynajrmu ontcsewiy,zsujy;jzpatmi aqmi&ujci;?
- vtyygu Subscriber rsm;u Refund ay;&e (ol) tpm;x; ouaocvurwrsm;xway;&e pp0aqmi&ujci;?
- CA \ Private Key Ei Hardware Token rsm; Disposition jy\vyjci;?
- CA \ 0eaqmir (Services) rsm;u qucrntjcm; CA ovajymi;ay;ty&eaqmi&ujci;?
- vyie;v;0&yprnae&uEi &yprntptp0u Root CA owijyjci;? Root CA r MOSS CA \ouaocvurwuy,zsujci;Ei vtyyguim;&r;o;porsm;\ ouaocvurwrsm; uyg y,zsujci;/

6. en;ynmqi&m vjcla&; xe;cyrrsm; (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 ,\unpwc\&on pepu to;jyjci;? Key rsm;u owrw xm;aom Cryptographic t&ntao;twi; jy\vyjci;Ei Private Key rsm;u rouqiorsm;r to;jyjci;? jyjyiajymi;vjci;? xwazmajymqjci;? aysmuq;jci; tp&onwr umu,jci;rsm;u aqmi&uxm;yg on/ MOSS CA \ Key generate jy\vyjci;u \ulwia&;qxm;on Key Generation Ceremony twi; aqmi&uxm;yg on/

im;&r;o;porsm;twu Key Pair tm;v;u \ulwiowrwxm;on owrwcsursm;twi; Generate jy\vyygon/ Key Generate jy\vyonvyie;p0u jyiy Network Ei Internet cswquxm; jci;r&aom o;oeowrwxm;on uey\wmwiomjy\vyygon/ CA Key Pair Generation Eiou

qionvyie; (Activities) tm;v;u ae&u ? tc:eEiwu rwwr;xm;&y; yg0ivyaqmio tm;v;r vurwa&;x;yg on/ prtyc:yor owrwxm;onumvtx xrwwr;rsm;u vty ov ppaq;jci; (Audit) ? jyevn:un&rrsm; (Tracking) jy:vyEi&e or;qn;xm;yg on/

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

(Private Key Delivery to Subscriber)

RA Ei Subscriber rsm;\ Key Pair rsm;u MOSS CA r Generate jy:vyyg u Handware Token (o:) Device rsm;u vjc:pwc:&aomen;o;í ay;yjzea0rnjzpyg on/ Device u Activate jy:vy&e vtyaom Data u RA (o) Subscriber o ay;yyg on/ xo ay;yjci;rsm;uvn; rwwr;xm;& yg on/

MOSS CA r Key Pair xway;yg u Private Key uouaocvurwtrs;tpm; (Class 2, Class 3) twuim;&r;o;pou,wi RA &;o vma&muí xw,&e vtyyg on/

6.1.3 CA \ Public Key u Relying Parties rsm;rto;jy:Ei&e pp0aqmi&uxm;jci;

(CA Public Key Delivery to Relying Parties)

MOSS CA \ ouaocvurwEi im;&r;o;porsm;\ ouaocvurwtm;v;u ,i; CA \ Website www.moss.com.mm wi Download jy:vyEi&e wixm;yg on/ im;&r;o;porsm; ouaocvurw& Certificate Chain wi Root CA Ei MOSS CA ouaocvurwtyg t0i Full Certificate Chain tm;v; yg0irn jzpyg on/ S/MIME Protocol u to;jy:aom Relying Party rsm;Ei ouaocvurw to;jy:orsm;on 4i;w& MOSS CA ouaoc vurw\ Validity u o&&e Certificate Hash Value u Website & Hash Value Ei wuqippaq;&rn/ MOSS CA ouaoc vurwu Root CA \ National Repository www.rootca.org.mm/repository wivn; azm:yxm;rn jzpyg on/

vtyyg u Root CA Ei MOSS CA \ ouaocvurwrsm;u Download jy:vyí rr\ Computer wi Install jy:vyEiyg on/

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

Key-Pair rsm;\ Private Key rsm;u Cryptanalysis jy:vyjci;en;jzi o&atmijy:vyEijci;r umu,Ei&etwu vavmuaom Key t&n (Key Length) xm;&yg on/ MOSS CA \ Key Lenght rm (2048) Bit RSA jzpyg on/ RA Ei im;&r;o;porsm;\ Key Pair Size on (1024) Bit jzpyg on/ vurwa&;x;&etwu to;jy:aom Hash Algorithm rm SHA1 jzpyg on/

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

(Public Key Parameters Generation and Quality Checking)

ouqijci;r&yg/

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

MOSS CA \ Key uatmuyg&n&,curm;jziom to;jyygon/

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

6.2 Private Key umu,jci;Ei Cryptographic Module o;pxe;cdyjci;rm;

(Private Key Protection and Cryptographic Module Engineering Controls)

MOSS CA on Physical, Logical Ei Procedural Control rm;aygi;pyum ,i; \ Private Key rm;u trewu,vcdpwcr&ape praqmi&uxm;&ygon/ ouaocvurw im;&r;o;porm; tm; rr\ Private Key jyiqic&ci; ? aymuq;jci; ? owpyg;rto;jyjci;rm; ? tjcm;orm;tm; xwazmajymumjci; (Disclosure) rm;u umu,&evtyaom ;uwiumu,rrm; jy|vy&e toay;xm;ygon/

6.2.1 Cryptographic Module \ t&n tao;pEi xe;cdyrrm;

(Cryptographic Module Standards and Controls)

MOSS CA on pepvjcdrltwu Key Generate jy|vyjci;Ei Key Storage twu FIPS 140-1 (Level-3) tqi&on Hardware Security Module u to;jyygon/

6.2.2 Private Key u vtrm;xe;cdyr| (Private Key (m out of n) Multi-Person Control)

jyXme;xm;jci;r&yg/

6.2.3 Private Key Escrow jy|vyjci; (Private Key Escrow)

jyXme;xm;jci;r&yg/

6.2.4 Private Key Backup jy|vyjci; (Private Key Backup)

MOSS CA on 4i;\ Private Key rm;u obm0ab;tE&m,ua&mujy;aomtcg vyie; quvuaqmi&uEi&e (Recovery jy|vy&e) twuom þ CPS ygowrwcurm;twi; Backup

Copy xm;&ygon/ x Key rsm;u v\0uu' (Encrypt) jy\vyí 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; rjy\vyEi&e vtyaom Procedural Control rsm;xm;&ly; HSM wi or;qn;xm;&ygon/ rwwr;a[mi;tjzp or;qn;xm;on ouwr; (5)Ep ausmom;ygu þ CPS wia&;om;xm;ontwi; v\cpmzsuq;ypygon/ ouwr;ueom;aom CA Certificate rsm;u ouwr;xyrrw;awmygu x Key Pair rsm;uo;í Sign x;jci;rjy\vyawmyg/

6.2.6 Private Key u Cryptographic Module xwi (o) Cryptographic Module r ajymi;a&\jci; (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 utjcm;aom Hardware Cryptographic Module o Backup tjzp ajymi;a&\ygu Encrypt jy\vyxm;on ypjziom wpcrwpco ajymi;a&\jci; 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\jyic&jci; ? tcir&orsm;r o;pjci; ? zi\unjci; r&ap&e Activation Data u umu,jci;rsm; 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; yg0ijy\vyrom atmijriaprn jzpygon/

Class 1 Private Key rsm; ? Class 2 Private Key rsm;Ei Class 3- Private Key rsm;u umu,rjy\vy&etwu powrwcsurm- Subscriber to;jy\aom Workstation Ei Private Key u

tjcm;orsm; 0ia&muo;pjci;rjy\vyEi&e vtyaom &yyi;qi&mwm;q;umu,rrsm; jy\vyxm;&yg on/ 4i;tjyi MOSS CA on Subscriber rsm;tm; ty' (6.4.1) wi azmjyxm;ontwi; Password u to;jy\&e (o) tvm;wvjc\r&aponen;rsm; to;jy\ygon/ (Private Key u to;jy\&e Password xm;&jci;? Windows Login (or) Screen Saver Password (o) Network Login Password rsm;to;jyjci;) rsm;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;p0 wiyg0icaom Trusted Person r Manual Shut Down jy\vyjci;? Log Out jy\vyjci;jzi Private Key u Deactivate jy\vyygon/ ouaocvurwim;&r;o;porsm;on rrvyie;aqmi&ujy;ontcgwi; CPS wiazmjyxm;ontwi; rr Private Key u Deactivate vy&e wm0e&ygon/ RA Ei ouaocvurwim;&r;o;porsm;on rrvyie;aqmi&ujy;ontcgwi; rr Private Key u Deactivate vy&e? e-Token u z,&m;jci; (o\) Certificate Store & Key File rsm; zsucjci; wujy\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&xwrvtajctae (Factory Initial State)o ajymi;vjci;en;jzijyevn wnaqmuo;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 ony,zsujci;rc&ygu (3) Epjzpygon/

xtjyi CA on ¤i;\ ouaocvurwouwr;rueq;r (1) Ep lulwií ouaoc vurw topxway;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 (6) – 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)

MOSS CA Ei ouaocvurwim;&r;o;porsm;on rrw\ Private Key u umu,&e vlcpwcs&on Strong Password (o) Activation Data (Secret Shares) rsm;to;jy\&rn jzpygon/ Secret Share rsm; Create jy\vyjci;? zsuq; (Destroy) jy\vyjci;rsm;u Log File jzirwwr; xm;&ygon/ Password a&;cs,jci;twu nelum;csursm;rm -

1/ to;jy\o (User) r Generate jy\vy&rn/

2/ ten;q; Character (8) v;&&rn/

3/ ten;q; tu&m (Alphabetic) (1) v;Ei *Pe;eygw (1) c yg&&rn/

4/ ten;q; Lower Case Character (1) v;yg&&rn/

5/ Character (1) v;wn; t\urrsm;pm xyumxyum yg0ijci;rjy\&/

6/ Operator \ Profile Name Eiwnrr&&/

7/ to;jy\o (User) \trnxr rnontpwtyi;?emrnw0uwysu yg0ijci;r&&/

MOSS CA on im;&r;o;porsm;tm; Authentication jy\vy&mwi en;(2)en; (Two Factor Authentication) (eg. Token & Passphrase, Biometric & Token, Biometric & Passphrase) wo;í Private Key Activation uumu,&etujy\wuwe;ygon/

6.4.2 Activation jy\vy&mwi o;aomtcsutvursm;u umu,jci;

(Activation Data Protection)

MOSS CA Ei RA \0exr;rsm;on rr\ Shared Password u rrbmomvlcatmi xe;or;&eEi xuoxe;or;onorsm;\ wm0e0w&m;rsm;u o&em;vnygalumi; oabmwn csuwi vurwa&;x;xm;&rn/

CA rsm;\ Administrator rsm;?0exr;rsm;?im;&r;o;porsm;on rr\ Private Key u Encrypt jy\vyí Password Protection jzixe;or;xm;&&rntjyi¤i;w Browser wi "High Security" Option xm;&ay;&rn/ Administrator rsm;? RA Ei im;&r;o;porsm;on 4i;w\ Private

Key u Encrypt jyvyí Hardware Token u to;jyjci; (o) vcr&on Passphrase rm; to;jyjci;jzi or;qn;xm;&rn/ Two factor Authentication u to;jy&e tm;ay;wuwe;ygon/

6.4.3 Activation jyvy&mwi o;aomtc;utvurm;Ei ouqiaomtjcm;talumi;t&m rm;

(Other Aspects of Activation Data)

6.4.3.1 Activation jyvy&mwi o;aomtc;utvurm;ay;yjci;

(Acitvation Data Transmission)

Private Key \ Activation Data u ay;y&mwiaymuq;jci; ? c;,c&jci; ? jyjyic&jci; ? tci r&bzi[ajymqjci; (Disclosure) ?w&m;r0ito;jyjci; (Unauthorized Use) rc&ap&e umu,&rn/ Window Ei Network Logon User Name Ei Password u wzuíim;&r;o;porm;\ Activation Data tjzpto;jy&mwi Network rwqi ay;yaom Password u rouqiaom User rm;rto;jyjci;r&ap&eumu,&rn/

6.4.3.2 Activation jyvy&mwio;aomtc;utvurm;zuq;jci;

(Activation Data Destruction)

Activation Data rm;u to;jyí Private Key u aymuq;jci; ? c;,c&jci; ? jyjyic&jci; ? tcir&y zi[ajymqjci; (Disclosure) ? w&m;r0ito;jyjci; (Unauthorized Use) r&ap&e pr aqmi&uxm;ygon/ Activation Data rm;u rwwr;xe;or;onumv aumveí zuq;ontcg Overwriting jyvyjci; (o) trewu,zuq;jci; en; (2) rs;v; (o) wprs;rs;uo;ípepwus zuq;ygon/

6.5 ueyswmpepvjcla&; xe;cyrrm; (Computer Security Controls)

CA Ei RA vyie;rm;twu ,lunpwc&onpepu A[tzEi lu;luyrtz w\ oabmwnc;ujzi owrwxm;on vjcla&;qi&m nelum;curm;Eitn uunr&atmi aqmi&uxm;ygon/

6.5.1 ueyswmvjcla&;twu en;ynmqi&m o;jcm;vtyc;urm;

(Specific Computer Security Technical Requirements)

MOSS CA on 4i;\ CA Software Ei Data File rm;u rouqiorm;r Access rjyvyEi &e ,lunpwc&on pepxm;&ygon/ xtjyi Key Generate jyvyaom Computer ? CA vyie; rm;Ei ouqion Database rm; ? Server rm;tm; wu&uuiw,o;pEiciu owrwxm;& on ,lunpwc;orm;uom ciay;xm;jy;civaom Business talumi;jyc;ujziom o;pcijyyg on/ General Application User rm;twu Production Server wi Account rxm;&y/

CA \ Production Network u tjcm; Components rsm;Eio;jcm;jzpap&e (Logically Separated) aqmi&uxm;ygon/ Network Access uvn;umu,xm;ygon/ CA on 4i;\ Production Network u twi;yi; (Internal) Ei tjyiyi; (External) us;ausm0ia&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;u ajymi;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) Eitn aqmi&uxm;ygon/

RA rsm;on Network u twi;yi; (Internal) Ei tjyiyi; (External) us;ausm0ia&mujci; rjy(vyEi&eei Firewall u to;jy(í umu,xm;ygon/ Network Activities rsm;\ oabmobm0 (Nature) Ei Service uueowjci;rsm;uvn; praqmi&uxm;ygon/ RA rsm;on Password to;jy(rEipyv(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; xo o;p&ermvn; civaomtalumi;jyc(u (Business Reason) &&rn jzpygon/

6.5.2 ueys(wm vjcla&;tqitajctae (Computer Security Rating)

vtyovjyXme;ygon/

6.6 en;ynmqi&m jzpp0rsm;xe;cs(yr (Life Cycle Technical Controls)

vtyovjyXme;ygon/

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

MOSS CA Ei RA on ¤i;\ vyie;rsm;tm;v;u rouqiorsm;r 0ia&muírormrrsm; rjy(vyEi&e vlcpwc(&on Network pepxm;&jy; Security and Audit Requirement Guideline rsm;twi;aqmi&uygon/ rouqiorsm;tm; lun&cirjy(aom Sensitive Information rsm;u tjyetveay;y&mwi Encrypt jy(vyíaomvn;aumi;? Digital Signature rsm; o;píaomvn; aumi; ay;yygon/

MOSS CA on vyie;aqmi&ujci;Ei jyfyixe;or;jci; (Operation and Maintenance) u Off Line jyfvyjy; tjcm;aom rnonueyfwmEi qupyypn;rsm;Eir ue,ucwquxm;jci; rjyfvyyg/

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

ouaocvurwrsm; ? CRL rsm;Ei tjcm;aom Revocation Database rwwr;rsm;wi vyaqmion tceEiae&uurwwr;xm;&yg on/ xuo tceqi&mrwwr;rsm;jyfvyjci; twu Cryptographic en;pep to;jy&erv 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 uunyg on/

terq;tqitm;jzi X.509 ouaocvurwrsm;wi atmuazmjyygrsm;yg0iyg on/

(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) jzpyg on/

7.1.2 ouaocvurw Extension rsm; (Certificate Extensions)

vtyovjyXme;yg on/

7.1.2.1 Key Usage

X.509 Version(3) ouaocvurwrm;on RFC 5280 owrwcurm;twi; xnoi; xm;yon/ X.509 Certificate rm;\ Key Usage Extension u atmuazmjyyZ,m;wi azmjyxm;ontwi; Set and Clear jy\vyyon/ Key Usage Extension Criticality Field ua,b,s 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 (7) – Settings for KeyUsage 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

v t y o v j y X m e ; y g o n /

7.1.2.6 CRL Distribution Point

Relying Party r s m ; r CA o u a o c v u r w r s m ; \ t a j c t a e u p p a q ; E i & e t w u End User Subscribes r s m ; \ CRL Distribution Points Extension w i CRL File u www.moss.com.mm/download/moss.crl r download v y E i y g o n /

7.1.2.7 Authority Key Identifier

CA o n i m ; & r ; o ; p o r s m ; \ X.509 Version-3 o u a o c v u r w r s m ; \ Authority Key Identifier Extension w i o u a o c v u r w u x w a y ; a o m CA \ Public Key u x n o i ; a z m j y x m ; y g o n /

7.1.2.8 Subject Key Identifier

CA o n X.509 Version 3 o u a o c v u r w r s m ; \ Subject Key Identifier Extension w i o u a o c v u r w u i a q m i t w u x w a y ; x m ; a o m Public Key u x n o i ; a z m j y x m ; y g o n /

7.1.3 Algorithm Object Identifiers

CA o n Certificate r s m ; u a t m u a z m j y y g Algorithm t o ; j y \ í Signing j y \ v y y g o n /

SHA-1 with RSA Encryption u t o ; j y \ y g o n /

7.1.4 t r n a y ; y p (Name Forms)

CA o n o u a o c v u r w r s m ; \ Issuer E i Subject Distinguish Name w i t y ' (3.1.1) w i a z m j y x m ; o n t w i ; j z n o i ; y g o n /

7.1.5 o u a o c v u r w t r n a y ; j c i ; q i & m o w r w c s u (Name Constraints)

MOSS CA o n Anonymous Name r s m ; u c i r j y \ y g / t r n r s m ; o n t " y m , & & r n t j y i i m ; & r ; o ; p o \ t r n E i v n ; y w o u r & & r n / t r n r s m ; o n Unique Distinguished Name (DN) j z p & y g r n /

7.1.6 ouaocvurw\r0g'qi&m u,pm;jy|c:u (Certificate Policy Object Identifier)

Certificate Policy Extension **u t o;jy|yg u ouaocvurwr:m;wi 4i;w\ tr:;tpm;tvu ty' (1.2) wi azmjyxm;onEi t n** CP **** Object Identifier (OID) **xnoi; azmjyay;xm;yg on/**

7.1.7 r0g'qi&m to;jy|r (Usage of Policy Constraints Extension)

jyXme;xm;jci;r&yg/

7.1.8 r0g' t&n tao;ypEi a0g[m&t"ym, ziqc:u

(Policy Qualifier Syntax and Semantics)

v t yo v jyXme;yg on/

7.1.9 ouaocvurw\ ta&;|u;aom r0g'qi&m a0g[m&t"ym,r:m;u aqmi&ujci;

(Processing Semantics for the Critical Certificate Policies Extension)

jyXme;xm;jci;r&yg/

7.2 CRL Profile

CRL **wiatmuazmjyygZ,m;twi;** Basic Field **r:m; yg0iygon/**

Field	Value or Value Constraint
Version	X.509 Version 2 CRLs.
Signature Algorithm	Algorithm used to sign the CRL: SHA-1/SHA-256 (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 (8) CRL Profile Basic Fields

7.2.1 Version Number (S)

CA on X.509 Ei Version 2 CRLs rsm;u (Support) jy\vyygon/

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&urypt m;lu;luyrEi A[tzw oabmwnxm;on Security Ei Technical Guideline wiazmjyxm;on tcsutvursm;twi;lu;luyrtzr vtyov ppaq;r jy\vyrnjzpygon/ Root CA Ei lu;luyrtzw\ Compliance Audit jy\vy&&rtay:wi rwní nelum;on twi;jznqn;aqmi&uom;rn jzpygon/

x\tjyi CA on 4i;\,lunpwcs&aompepu aocsmr&ap&etwu jyevnppaq;jci; Ei ppr;ppaq;jci;jy\vy&mwi ten;q;atmuygwyg0iygon/

- vjcla&;Ei vyx;vyen;rsm; jyevnpppjci; (vjcla&;qi&mpm&upmwr;rsm; ? CP/CPS ? CA Eiouqiaomoabmwpmcsyrsm;) ?
- MOSS CAonatmuyg tajctaersm;jzpay:v\i4i;\pepupm&i;ppjci;jy\vy&rn/
  - CA \pepEi Root CA \pm&i;ppjci;rsm;wi owrwxm;aom prsm;ei uunrr&onu aw\&&jci; ?
  - rawmwqxcurrsm; (o) cs\;azmuc&rrsm; jzpay:jci; ?
  - CA pep\vjcla&; (o) Integrity u ysup;Eiacs&aom uprsm;jzpay:jci; ?
- CA on vtyygu Risk Management uaqmi&u&rn/

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

- Root CA onouaocvurwxway;yici&o CA rsm;u (1) Epwi (1) lur en;ynm qi&mpm&i;ppjci;jy\vyygon/
- pm&i;ppjci;rsm;u lu;luyrtzr vucaom t&ntcsi;jyn0on pm&i;pptzrsm;Ei ppaq;ygon/ pm&i;pptzwi vurw&pm&i;uiwp0;Ei Certified Information System Auditor wp0;yg&rnjzply; wp0;0;on'p*spw,ouaocvurwrsm;Ei,i;wEi ywou aom toynm?A[ow&ojzp&rn/
- CA rsm;on rrpeptwi; Internal Audit u wpEpv\i (2) lur ppaq;jci;jy\vyygon/

8.2 tm;en;cu (o) v tycurm;ay:rwní vyaqmicu

(Action Taken as a Result of Deficiency)

MOSS CA on pm&i;ppjci; ppaq;cut& v tycurm;? ›ci;cuEi tm;en;curm; &yu lu;luyrtzEi Root CA r nelum;ontwi; jznqn;aqmi&uygon/ ›ci;cu ? tm;en;curm;tay:rwní ta&;,rn Action u MOSS CA \prtycsyrtzrq;jzwygon/ MOSS CA \ tycsyrwi wm0e&orm;on Corrective Action Plan u taumitxnazm&e wm0e&ygon/ tu,í x›ci;cuEiv tycurm;on MOSS CA \ Security Ei Integrity u lcr;ajcmu xcuaprnqygu CA r Corrective Action Plan u &u (30) twi; a&;qí oiavsmaom tcsetwi; taumitxnazmrnjzpygon/ Serious Exceptions r[won Deficiencies rm;twu MOSS CA r xtcsu\ ta&;yguru wucsuí oiavsmaom ta&;,ru q;jzwrn jzpygon/

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

(Other Business and Legal Matters)

9.1 ay;oi;&rnaialu; (Fees)

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

(Certificate Issurance (or) Renewal Fees)

im;&r;o;porm;r ouaocvurwxw,jci; ? ouwr;w;jci;Ei ouaocvurw prcecjci;qi&mwtwu usoiaiu CA (o) RA rm;o ay;aqmi&ygrn/

9.1.2 ouaocvurwu lun&jci;twu usoiai (Certificate Access Fees)

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

9.1.3 ouaocvurwy,zsupm&i;Ei tajctaeu lun&jci;twuusoiai

(Revocation or Status Information Access Fees)

MOSS CA on Certificate Revocation List (CRL) xwjyejci;? x CRL u Relying Party rm;r lun&Ei&ejylvyay;jci;wtwu usoiaiaumucrnr[wyg/ olaomtjcm;aom Value-Added Revocation Information 0eaqmirrm;twu usoiaiaumucrnjzpygon/ CA on tjcm;aom Third Party rm;r Revocation Information rm; ? Certificate Status Information rm; (o) Repository wi Time Stamping jylvyjci;rm;u CA r ouqi&mwm0ec\pmjzi a&;om;cijylxm;jci; r&yu cirjylyg/

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

MOSS CA on CP Ei ,i;Eiouqiaom þ CPS u Access vyjci;twuusoiai aumucjci; r&yg/ Document rsm;u lun&&r\r[wb jyevnxwa0jci; (Reproduction) ? jyiqijci; (o) ,i;wu to;jy\í tjcm;aomvyie;rsm; quvuvyuijci;uoaom tjcm;aom &n&,csursm;jzito;jy\vygu Document rsm;u ryici (Copyright) &o MOSS CA Ei oabmwncsu &,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;csrwíouaoc vurwxway;jci;qi&mvyie;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 xoawmi;qvmaomtcg atmuygtwi; jyetr;aiu xway;ygon/

- Class 3- Type-A ouaocvurwwpapmiv\i
  - tp;&Xmeqi&mrsm;twu usy (15,000) jzpygon/
  - y*vuqi&mrsm;twu usy (20,000) jzpygon/
- Class 3- Type-B ouaocvurwwpapmiv\i
  - 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,yitptp0jzi 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&e twu vavmuaom aialu;&ygon/

9.2.3 tjcm;aom tmrcwi yg0irrsm; (Extended Warranty Coverage)

jyXme;xm;jci;r&yg/

9.3. p;ym;a&;qi&m tcutvursm;uvw0ujci; (Confidentiality of Business Information)

9.3.1 vw0utjzpowrwxm;aom tcutvursm; (Scope of Confidential Information)

MOSS CA on im;&r;o;porsm;\atmuazmjyyg tcutvursm;u vw0utcutvu rsm; (Confidential and Private Information) [owrwygon/

- ouaocvurwavmuxm;jci;qi&m tcutvursm; 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;Ei tp&icpmrsm;?
- Contingency Plan Ei Disaster Recovery Plan rsm; ?
- Hardware, Software rsm;\vyie;aqmi&ur (Operation) \vjcla&;xe;cslyrrsm; ? ouaoc vurw0eaqmiray;jci;\ vyie;prtycsyrqi&mrsm;Ei owrwxm;aom pm&i;a&;oi; jci;qi&m0eaqmirrsm;Ei ywouon tcutvursm; ?

9.3.2 vw0utcutvursm;[owrwxm;aom tcutvursm;

(Information not within the Scope of Confidential Information)

ouaocvurwrsm;? ouaocvurwy,zsujci;Ei tjcm;ouaocvurw\tajctae (Status) qi&m owi;tcutvursm;? MOSS CA Repository Ei 4i;twi;& owi;tcutvu rsm;u vw0uEi y*lva&;qi&m tcutvursm; (Confidential and Private Information) tjzp rowrwyg/ þ CPS yg tcursm;on trsm;jynou lun&ci ? o&ciay;xm;aom tcutvu (Non-Confidential) rsm;jzpygon/ 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;u umu,&ewm0e,aqmi&ur

(Responsibility to Protect Confidential Information)

MOSS CA on tjcm;aom rouqiorsm; (Third Parties) r vw0uEiy*lva&;qi&m tcutvu (Confidential/ Private Information) rsm;u cs;azmu0ia&mulun&jci; rjylvyEi&e praqmi&uxm;ygon/

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

(Privacy of Personal Information)

9.4.1 y*lva&;qi&m tcutvu v0ujci;prcu (Privacy Plan)

MOSS CA Ei RA rm;on wp0;wpa,muEiqion u,a&;tcutvurm;u vjcr &atmi aqmi&u&etwu nelum;curm;Ei uunr&aom Privacy Policy u a&;qaqmi&u xm;ygon/

9.4.2 u,a&;v0utjzpourwontcutvurm; (Information Treated as Private)

ouaocvurwavlmuxm;oEi ouqiontcutvurm;xr CA r xway;on ouaocvurwrm; ? ouaocvurw Directory rm; ? On-Line CRL wi azmjyxm;on rm;rví useaomtcutvutm;v;u u,a&;v0utcurm;[owrwygon/

9.4.3 u,a&;v0ur[w[totrwjylxm;aom tcutvurm;

(Information Not Deemed Private)

trm;jynolun&Eion ouaocvurwwiazmjyxm;on tcutvurm;u u,a&; v0utcutvurm;[rowrwyg/

9.4.4 u,a&;v0utcurm;uumu,&ewm0e,rrm;

(Responsibility to Protect Private Information)

CA/RA Ei 4i;\ Participant tm;v;on vuc&&xm;on v0utcutvurm;u cs;azmulunc&jci; (Compromise) Ei tjcm;rouqiotztpn;rm;x ay;yjci; ? azmjyjci; rjzpap&e umu,xm;ontjyi w&m;p&iyicit& jynwi;& jyXme;xm;aom0ya'rm;twi; uunr&ap&evn; aqmi&uxm;ygon/

9.4.5 u,a&;tcutvurm;uto;jy&etwutalumi;lum;jci;Eioabmwncu

(Notice and Consent to Use Private Information)

þ CPS wiy&on u,a&;tcutvurm;u ouqion Privacy Policy (o) avlmuxm;o\oabmwncur&&cvli to;jylrnr[wyg/ þ tyi;on Privacy qi&mumu, xm;&&rn owrwcurm;twi;jzpygon/

9.4.6 w&m;p&ia&; (o) prceca&;qi&mvyie;pOrsm;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&m uprsm;Ei tjcm;aomw&m;a&;qi&mv tyaomvyie; (Legal Process) rsm;twu lu;luyrtz\ cijyicsujziom azmxwjyoci&ygon/

9.4.7 tjcm;aom tcsutvursm;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;&n yiqiciqi&mtcita&;ay;jci; (IPR) (o) xojyivyay;&e tcitmPmEiwm0er&yg/ þ CPS r u;,aomrnontalumi;t&mrq þ CPS r u;,alumi;u;um;csu ?&nne;csu yg&&rn/

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

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

9.6 u,pm;jyirrsm;Ei tmrccsursm; (Representations and Warranties)

9.6.1 MOSS CA rwm0e,rntcsursm; (CA Representations and Warranties)

MOSS CA ratmuygtcsursm;Ei pyvs0;ívavmuaomaocmr&&rn/

- MOSS CA r xway;xm;aomouaocvurwavimuvmrsm; (oi) xway;iy;aom ouaocvurwrsm;r tcsutvursm;u rm;,i;pmazmjyjci; (Misrepresentation) r&&yg/
- ouaocvurwavimuxm;jci; (Certificate Application) (o) ouaocvurwjyivyjci; wu praqmi&u&mü ouaocvurwr tcsutvu (Information) rsm;u ouaoc vurwavimuxm;jci;u twnjyio (o) ouaocvurwjyivyo\ owcsi,i;ralumi trm;rsm;ryg&ap&yg/

- MOSS CA r xway;aomouaocvurwrsm;on þ CPS Ei CP wiyg&aom vtyaom owrwcsursm;tm;v; (All Material Requirement) Ei uunr &ygon/
- ouaocvurwy,zsujci;Eiqiaom 0eaqmirrsm; (Revocation Services) Ei Repository to;jyron þ CPS Ei CP rsm;& owrwcsursm; (Material Aspects) tm;v;Ei uunr &ygon/

9.6.2 RA rwm0e,rn tcsursm; (RA Representations and Warranties)

RA ratmuygtcsursm;Ei pyvs0;í vavmuaomaocsmr&&rn/

- ouaocvurwavmuvmrsm; (o) xway;y;aomouaocvurwrsm;r tcsutvu rsm;u rm;,i;pmazmjyjci; (Misrepresentation) r&&yg/
- ouaocvurwavmuxm;jci; (Certificate Application) (o) ouaocvurwjymvy jci;wu praqmi&u&mü ,i;\azmjyygtcsutvu (Information) rsm;u avmuxm; jci;utwnjyo (o) ouaocvurwjymvyo\ owcs,i;ralumi trm;rsm;ry&ap&yg/
- ouaocvurwrsm;on þ CPS Ei CP wiyg&aom vtyaomowrwcsursm;tm;v; (All Material Requirement) Ei uunr &ygon/
- ouaocvurwy,zsujci;Eiqiaom 0eaqmirrsm; (Revocation Services) Ei Repository to;jyron þ CPS Ei CP rsm;&owrwcsursm; (Material Aspects) tm;v;Ei uunr&yg on/

9.6.3 ouaocvurwavmuxm;orwm0e,&rntcsursm;

(Subscriber Representation and Warranties)

ouaocvurwavmuxm;or tmrc&rntcsursm;rm -

- ouaocvurwwiyg0ion Public KeyEi 4i;Ei ouqiaom Private Key uo;í a&;x;xm;aom Digital Signature wi;on ouaocvurwim;&r;o;po\ Digital Signature jzpon/ x Digital Signature uvurwa&;x;aecsewi4i; ouaocvurw onto;jyí&aom tajctaewi&jy; ouwr;ueq;jci; (Expired) (o) y,zsujci; (Revoked) vyxm;c&jci; tajctaers;rjzpap&yg/
- 4i;w\ Private Key uaocmpmxe;or;umu,xm;&rn/ rnoncijyrxm;aomo (Unauthorized Person) r ouaocvurwim;&r;o;po\ Private Key u,ío;pEijci; r&ap&yg/

- ouaocvurw av|muxm;oray;aom tc\utvursm; ? ouaocvurw av|muvm wia&;oi;aomtc\utvursm;Ei ouaocvurwwi azmjyxm;aom tc\utvursm; on reuer&&ygrn/
- ouaocvurwu þ CPS Ei CP wiyg&on cijy|xm;aom ? w&m;0iaom 0ya'qi&m &n&,c\ursm; (Authorized and Legal Purpose) twuom to;jy|ygrn/
- im;&r;o;poon rr\ouaocvurwtm; ouaocvurwxway;yici&o (CA) uo tjcm;aomouaocvurwrsm; ? CRL rsm;uvurwx;ay;jci; (Digitally Singing) rjy|vy&yg/

9.6.4 Relying Party rsm;rwm0e,rntc\ursm;

(Relying Party Representation and Warranties)

Relying Party rsm;on rr,lunrjy|on ouaocvurwEi 4i;wiyg0iaom ouaocvurwqi&mtc\utvursm;\ ppreru p0;pm;q;jzw&e vtya|umi; ? Relying Party Agreement wi a&;om;azmjyc\ursm;u em;vnyga|umi;Ei ? ,i;ouaocvurwu o;p&eoi ? roi q;jzw&e rrwiomwm0e&a|umi; em;vno&&rnjzpygon/

txupmy'wiazmjyxm;aom CPS yg Relying Party rsm;vuemaqmi&u&rnwm0ersm; (Obligation) u vuemrr&jci;a|umi 0ya'qi&mtu\;qursm;jzpay:vmygu ,i; Relying Party rwm0e,vuc&rn jzpygon/ MOSS CA \ ,lunpwcpmo;porsm;\ oabmwnc\u (Relying Party Agreement) wi tjcm;aom azmjyc\ursm;Ei tmrcc\ursm;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&,c\ursm;t& ouaocvurwo;porsm; oabmwnc\u (Subscriber Agreement) Ei Relying Party Agreement rsm;on MOSSA CA \ jzpEior| Warranties tm;v;u (Warranity of Merchantability (o) &n&,c\u wpctwu oiawmru tu\;0iaom rnon Warranty r\;urq) jii;y,Eion/ xjyi aygqr (Negligence) or[w vucEiz,&aom owrjci;r&r (Lack of Reasonable Care) w|tjyi CRL wiazmjyxm;aom

qi;i ? y,zujy;om; ouaocvurwrsm;tm; o;pjci;alumi jzpay:vmaom tus;qursm; twu rnonay;&ewm0e (Liability) urq MOSS CA rjii;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) ponwalumi jzpay:aom ysup;q;&;rrsm;u vn;aumi; ? ppyrsm;Ei obm0ab;tE&m,rsm;alumijzpay:aom ysup;rrsm; twuvn;aumi; avsmalu;aiay;jci; rjylvyy/ MOSS CA r Certificate trs;tpm;wpc ysup;q;&;rtwu ay;avsmrrsm; (Liabilities) u trsm;q; atmuygtwi; owrwxm;ygon/

Class	Liability
Class-3 (Type A)	- 60000 usy
Class-3 (Type B)	- 30000 usy

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

9.9 avsmalu;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;csursm;Ei &ypjci; (Terms and Termination)

9.10.1 pn;ur;csu (Term)

þ CPS on MOSS CA \ Repository wi Publication jylvyonaerpí w&m;0i (Effective) ygon/ þ CPS wi jyiqirrsm;jylvyygu xjyiqirrsm;on Repository wi Publish jylvyonaerpí tus;oua&mur&ygon/

9.10.2 &ypjci; (Termination)

rlumcP þ CPS **wi jyiqirrsm;on** Version **topjyXme;jci;Ei ajymi;vr jy\vyjci; r&oí w&m;0i** CPS **jzpygon/**

9.10.3 &ypjci;tus;w&m;rsm;Ei vyie;quvu&ywnjci;

(Effect of Termination and Survival)

þ CPS **u&ypvuaomvn;** CA **** Participant **rsm;on** Certificate **rsm;** Validity Period **jynonwiatmi x** CPS **ygtcsursm;twi; tus;0ir&ygon/**

9.11 wpO;csi;ptm;talumi;lum;jci;Eiquo,jci;

(Individual Notices and Communications with Participants)

vtyovjyXme;ygon/

9.12 jyiqirrsm; (Amendements)

9.12.1 jyiqirrsm;jy\vyonvyx;vyen;Ei Specification ajymi;vrnvyx;vyen;

(Procedure for Amendment/ Specification Change Procedure)

þ CPS **wi jyiqirrsm;u** CA Policy Management Authority **r jy\vyygon/ þ** CPS **wi jyiqirwi;u lu;luyrtz\ twnjycsu&,jy;rom jyiqijci; jy\vyygon/ jyiqirrsm;u a&;om;xm;on** Amended Form **pm&uypjzi4i;** ? Update **ypjzi4i; &Eiygon/ jyjyily;om;** CPS Version **rsm; (o)** Notices Section **wivn;** Link **ay;xm;rn jzpygon/ þ** CPS **wiajymi;vjci; jy\vyrrsm;on** CPS Object Identifier **rsm;wivn; ajymi;vrv ? rvu** MOSS CA **Ei** Root CA **\ prtycsyorsm;r q;jzwcsuay;ygon/**

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

MOSS CA **on** CPS **wi y&on pmyEyjci;qi&mtrm;rsm; ?** URL **ajymi;vrrsm; ? quo,&rnvypmajymi;vrrsm;ponwu\u\wi talumi;lum;&eEi\u;luyrtz\ twnjycsu&,&ew rvtyy jyjyiajymi;vci&on/ jyjyiajymi;vvonrsm;utlujycsuay;yEi&etwu tcseumvwpc owrwxm;ygon/ xjyjyiajymi;vrn tcsursm;Ei tlujycsursm;u** MOSS CA **** Website http://www.moss.com.mm **wiazmjyxm;ygon/**

9.12.3 OID ajymi;vjci;jy\vyrn tajctaersm;

(Circumstances under which OID Must be Changed)

vtyovjyXme;ygon/

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

MOSS CA **Eiouaocvurwim;&r;o;porsm;tlum;; y#yursm;jzpym;vmygu 4i;wEi** csyqxm;aom **oabmwncsursm;wi a&;om;xm;on** Dispute Resolution Procedure **rsm;twi; ajz&i;om;rnjzpygon/ vtyygu tvuxa&mep quo,aqmi&ua&;Oya' ? ta&;ay:prr Oya'rsm;ay:wi tajccí ay:ayguaomjyoem twi;twmt& tvuxa&mepquo,aqmi&u a&; A[tz ? lu;luyrtzlEi quo,a&;nelum;rO;p;Xmew\ vr;necursm;twi; ta&;, aqmi&uygon/**

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

þ CPS **wi ziqxm;on twi; bmomjyejci;** (Interpret) **? wnaqmujci;** (Construction)**? tmPmwnapjci;** (Enforceability) **Ei w&m;Oijzpjci;** (Validity) **rsm;Ei pyvsO;í jrermEii \ wnqOya'rsm;t&om aqmi&u&rnjzpygon/ jrermEii\ wnqOya'rsm;omv\i þ** CPS **u vr;r;onOya'jzpygon/**

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

þ CPS **on jrermEiiawmtp;&r jyXme;xm;on Oya'rsm; ? ouqion en;Oya'rsm;** (Regulations) **? pn;rsO;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 wmOeEi tcita&;rsm; xyqiay;tyjci; (Assigment)

þ CPS **wi ygOitusl;Oiorsm;on rrtm;ay;tyxm;on wmOeEitcita&;rsm;u** MOSS CA **\ oabmwcijycsur&b vajymi;ay;tyjci;rjy&/**

9.16.3 Oya't& ta&;,aqmi&uEir&apjci; (Serverability)

þ CPS **ygazmjycsu (o) jyXme;csu ? pn;ur;csuwpcEi pyvsO;í ay:ayguvmon tajctaewp&ywi w&m;&;awm** (Court of Law) **(o) tjcm;aom c&;rsm;wiwijyu;um;jci;rjylEi caomvn; xazmjycsu (o) pn;ur;csurví þ** CPS **\ usetpwtyi;rsm;on Oya't& quvuí tusl;oua&mur** (Valid) **&ygon/**

9.16.4 tmPmoua&mujci;(u,pm;v,?a&Uaetus;aqmicEipevwo\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;ponwm;q;ír&Eiaomup&yrsm;?obm0ab;tE&m,rsm;alumijzpay:vmaom ysup;q;&;rrsm;twu ay;avsm&ewm0er&yg?**

9.17 tjcm;aomlulwiprcsursm; (Other Provisions)

vtyov jyXme;yg on/

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

þ CPS **Eipyv0;ítlujycsu ? rwcsursm;ay;yvyg u þ** CPS **tm;** Publish **vyonaerpí (15) &utwi;** MOSS CA **xo talumi;lum;pmay;yEiyg on/** E-mail **rm** mossca@moss.com.mm **jzpyg on/**

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
RFC	Request For Comment
RSA	A Public Key Cryptographic System Invented by Rivest, Shamir, and Adelman
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 jzi 'a&;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;jyvyEi&e lu;luyrtzu tvuxa&mep quo, aqmi&ua&;0ya't& wm0eay;tyxm;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& xway;onvipiu &&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 omrevjclrvtycsursm; Eitn tzltpn;wpc or[w to;csr 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 tcseqi&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 trsm;jyno tv,wuEi tcrlun&Ei&e azmjyxm;on/ CRL rsm;u tcseqi&m rwwr;wijci; (Time Stamp) jylvyxm;ygon/

(Z) rwywixm;aom xway;yici&o (Registration Authority (RA)) qonrm ouaoc vurwavlmuxm;o\ talumi;t&mrsm;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;rjyyg/ (qvonrm RA wp0;on CA wp0;u,pm; wcswm0ersm;u aqmi &ujci;jzpon/)

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

(n) ouaocvurwavlmuxm;o (EndEntity) qonrm ouaocvurw xway;yici &o (CA) xr ouaocvurwwpcu awmi;qojzpon/

(#) ouaocvurwouwr;w;jci; (Certificate Renewal) qonrm ouaocvurwwi yg0iaom Public Key or[w wjcm; tcstutvursm;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/