Myanmar Info-Tech Corp. Ltd.

ROOT CERTIFICATION AUTHORITY

သက်သေခံလက်မှတ်ထုတ်ပေးခြင်းဆိုင်ရာ မူဝါဒများ

Certificate Policies

3RD MAY , 2010

Documentation Classification:

Public

(Version: 1.0)

Copyright © 2010 Myanmar Root CA , Republic of the Union of Myanmar. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes without prior written consent.

မာတိကာ

၁. နိဒါန်း (Introduction)

မြန်မာနိုင်ငံကို ခေတ်မီဖွံ့ဖြိုးတိုးတက်သော နိုင်ငံအဖြစ် တည်ထောင်ရာတွင် အီလက်ထရောနစ်နည်းဖြင့် လုပ်ငန်းများ လုံခြုံစိတ်ချစွာဆက်သွယ်လုပ်ကိုင်နိုင်ရန်၊ အီလက်ထရောနစ်ကူးသန်းရောင်းဝယ်ရေး (e-Commerce) နှင့် အီလက်ထရောနစ် အုပ်ချုပ်ရေး (e-Governance) တို့ဖွံ့ဖြိုးတိုးတက်လာစေရန် ရည်ရွယ်ချက်များဖြင့် အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေး ဥပဒေ (The Electronic Transactions Law) ကို ၂၀၀၄ ခုနှစ် ဧပြီလ ၃၀ ရက်နေ့တွင် ပြဋ္ဌာန်းခဲ့ပါသည်။ ထိုဥပဒေအရ အီလက်ထရောနစ် ဆက်သွယ် ဆောင်ရွက်ရေး ဗဟိုအဖွဲ့နှင့် အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေး ကြီးကြပ်မှု အဖွဲ့တို့ကိုလည်း ဖွဲ့စည်းတာဝန် ပေးအပ်ခဲ့ပါသည်။

အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေး ဥပဒေပုဒ်မ (၁၁) အရ သက်သေခံလက်မှတ် ထုတ်ပေး ပိုင်ခွင့်ရှိသူဆိုင်ရာလုပ်ငန်း လုပ်ကိုင်ဆောင်ရွက်ရာတွင် အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေး ကြီးကြပ်မှု အဖွဲ့ကို နည်းပညာဆိုင်ရာ အထောက်အကူ ပြုနိုင်ရေးအတွက် ကျွမ်းကျင်သော မြန်မာအင်ဖိုတက်ကော်ပိုရေးရှင်း လီမိတက်အား မူလအရင်းအမြစ်သက်သေခံလက်မှတ် ထုတ်ပေးပိုင်ခွင့်ရှိသူ (Root Certification Authority (Root CA)) အဖြစ် အောက်ပါလုပ်ငန်းတာဝန်နှင့် လုပ်ပိုင်ခွင့်များကို ဆောင်ရွက်ရန် ဗဟိုအဖွဲ့၏ သဘော တူညီချက်ဖြင့် ၂၀၀၈ ခုနှစ် သြဂုတ်လ (၁၄)ရက်နေ့ပါ စာအမှတ် ၃၂၇-ဆည/ခွဲ(၂)ရေး/၁၄၁၄ ဖြင့် တာဝန်ပေးအပ်ခဲ့ ပါသည်။ Root CA ၏ လုပ်ငန်းတာဝန်များမှာ အောက်ပါ အတိုင်းဖြစ်ပါသည်။

(က) အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေး ကြီးကြပ်မှုအဖွဲ့အား နည်းပညာပိုင်းဆိုင်ရာ ကိစ္စများတွင် တာဝန်ယူ ဆောင်ရွက်ပေးခြင်း။

(ခ) သက်သေခံလက်မှတ် ထုတ်ပေးပိုင်ခွင့်ရှိသူ သုံးစွဲရမည့် နည်းပညာစံချိန်စံညွှန်းများကိုလည်းကောင်း၊ ထိုသူထိန်းသိမ်းရမည့်စာရင်းတွင် မှတ်တမ်းတင်ထားရမည့် အသေးစိတ် အချက်အလက်များကိုလည်းကောင်း အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေး ကြီးကြပ်မှု အဖွဲ့မှ သတ်မှတ်နိုင်ရန်ပြုစုတင်ပြပေးခြင်း။

(ဂ) သက်သေခံလက်မှတ် ထုတ်ပေးပိုင်ခွင့်ရှိသူအဖြစ် ဆောင်ရွက်လိုသူကလုပ်ငန်း လုပ်ကိုင်ခွင့် လိုင်စင်လျှောက်ထားခြင်းနှင့် စပ်လျဉ်း၍ နည်းပညာအရ လိုအပ်သလိုစစ်ပြီး အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေး ကြီးကြပ်မှုအဖွဲ့သို့ သဘောထား မှတ်ချက် တင်ပြခြင်း။

(ဃ) သက်သေခံလက်မှတ် ထုတ်ပေးပိုင်ခွင့်ရှိသူ သုံးစွဲသည့် နည်းပညာသည် သတ်မှတ်ထားသည့် စံချိန်စံညွှန်းများနှင့် ကိုက်ညီမှု ရှိမရှိ အီလက်ထရောနစ်ဆက်သွယ်ဆောင်ရွက်ရေး ကြီးကြပ်မှုအဖွဲ့၏ ခွင့်ပြုချက်ဖြင့် စစ်ဆေးခြင်း။

(င) သက်သေခံလက်မှတ် ထုတ်ပေးပိုင်ခွင့်ရှိသူအား အရေးယူရန် လိုအပ်ကြောင်း နည်းပညာအကြောင်းပြချက်အရ စိစစ်တွေ့ရှိပါက အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေး ကြီးကြပ်မှုအဖွဲ့သို့ သဘောထားမှတ်ချက်ဖြင့် ဆောလျင်စွာတင်ပြခြင်း။

(စ) အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေး ဗဟိုအဖွဲ့နှင့် အီလက်ထရောနစ်ဆက်သွယ်ဆောင်ရွက်ရေး ကြီးကြပ်မှုအဖွဲ့တို့က အခါအားလျော်စွာ ပေးအပ်သည့် လုပ်ငန်းတာဝန်များကို ဆောင်ရွက်ခြင်း။

ဤစာတမ်းသည် မြန်မာနိုင်ငံတော် Root CA ၏ သက်သေခံလက်မှတ်ထုတ်ပေးခြင်း ဆိုင်ရာမူဝါဒများ (Certificate Policies(CP)) ဖြစ်ပါသည်။ ဤစာတမ်းတွင် Root CA မှ CA များသို့ သက်သေခံလက်မှတ်များထုတ်ပေးခြင်း၊ စီမံခန့်ခွဲခြင်း၊ ပယ်ဖျက်ခြင်း၊ သက်တမ်းတိုးခြင်းများ စသည်တို့ပြုလုပ်ရာတွင် Root CA ၏ သက်သေခံလက်မှတ် ထုတ်ပေးခြင်းဆိုင်ရာမူဝါဒများ ကို ဖော်ပြထားပါသည်။

ဤ CP သည် Internet Engineering Task Force (IETF) RFC 3647 ၏ Certificate Policies(CP) နှင့် Certificate Practice Statement (CPS) ရေးဆွဲရမည့် လမ်းညွှန်ချက်များအတိုင်း ရေးဆွဲထားခြင်းဖြစ်ပါသည်။ ဤ CP တွင် သုံးစွဲထားသော စကားလုံးများ၏ အဓိပ္ပါယ်သတ်မှတ်ချက်သည် အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေး ဥပဒေ(The Electronic Transactions Law)၊ ၎င်းနှင့်သက်ဆိုင်သော နည်းဥပဒေများ၊ အမိန့်ကြေငြာစာများအတိုင်း ဖြစ်ပါသည်။

၁.၁ အချက်အလက်အကျဉ်းချုပ် (Overview)

Root CA သည် မြန်မာနိုင်ငံအစိုးရမှ ခန့်ထားသည့် အဖွဲ့အစည်း ဖြစ်ပြီး Certificate Life Cycle ဝန်ဆောင်မှုများ (အသစ်ထုတ်ပေးခြင်း၊ စီမံခန့်ခွဲခြင်း၊ ပယ်ဖျက်ခြင်း၊ သက်တမ်းတိုးခြင်း) အားလုံးကို ဆောင်ရွက်ပေးပါသည်။ Root CA သည် လိုင်စင်ရ သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ (Licenced Certification Authority) များအတွက် သက်သေခံလက်မှတ် (Certificate) များကို ထုတ်ပေးပါသည်။

Root CA ၏သက်သေခံလက်မှတ်သည် မြန်မာနိုင်ငံတွင် အမြင့်ဆုံး သက်သေခံလက်မှတ်ဖြစ်ပြီး၊ မြန်မာနိုင်ငံရှိ CA များ ၏ public key များကို လက်မှတ်ရေးထိုးပေးပါသည်။ Root CA ၏ သက်သေခံလက်မှတ်သည် မိမိဘာသာ လက်မှတ်ရေးထိုးသော သက်သေခံလက်မှတ် (Self-signed Certificate) ဖြစ်ပါသည်။ ဤ CP ကို www.rootca.org.mm တွင် Download ပြုလုပ်နိုင်ပါသည်။

၁.၂ CP အမည်နှင့် အမှတ်အသား (Document Name and Identification)

ဤစာတမ်းသည် Root CA ၏ CP ဖြစ်ပါသည်။ ဤ CP ၏ Object Identification Value(OID)ကို Root CA၏ အကြံပြုတင်ပြချက်အရ ကြီးကြပ်မှုအဖွဲ့ မှအောက်ပါအတိုင်း သတ်မှတ်ပါသည်။
(၂ ၁၆ ၁၀၄ ၁ ၁ ၃)

၁.၃ PKI တွင် ပါဝင်သူများ (PKI Participants)

၁.၃.၁ ဗဟိုအဖွဲ့

ဤ CP တွင်ဖော်ပြထားသော ဗဟိုအဖွဲ့သည် အီလက်ထရောနစ်ဆက်သွယ်ဆောင်ရွက်ရေး ဥပဒေအရ ဖွဲ့စည်းထားသော အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေး ဗဟိုအဖွဲ့ ဖြစ်ပါသည်။

၁. ၃. ၂ ကြီးကြပ်မှုအဖွဲ့

ဤ CP တွင်ဖော်ပြထားသော ကြီးကြပ်မှုအဖွဲ့သည် အီလက်ထရောနစ် ဆက်သွယ် ဆောင်ရွက်ရေး ဥပဒေအရ ဖွဲ့စည်းထားသော အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေး ကြီးကြပ်မှုအဖွဲ့ဖြစ် ပါသည်။

၁. ၃. ၃ မူလအရင်းအမြစ်သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ (Root Certification Authority)

မူလအရင်းအမြစ်သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ (**Root Certification Authority(Root CA))** သည် အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေးကြီးကြပ်မှုအဖွဲ့ကို နည်းပညာဆိုင်ရာ အထောက်အကူပေးရန်၊ သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ(CA)များသို့ သက်သေခံလက်မှတ်များ ထုတ်ပေးခြင်း၊ သက်တမ်းတိုးခြင်း၊ ပယ်ဖျက်ခြင်း၊ စီမံခန့်ခွဲခြင်းများ ပြုလုပ်နိုင်ရန်အတွက် အီလက်ထရောနစ်ဆက်သွယ် ဆောင်ရွက်ရေး ဥပဒေအရ ကြီးကြပ်မှုအဖွဲ့က အမိန့်စာဖြင့် တာဝန်ပေးခန့်အပ်ထားသော အဖွဲ့အစည်း ဖြစ်ပါသည်။

၁. ၃. ၄ သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ (Certification Authorities(CA))

CA များသည် Root CA မှထုတ်ပေးသော သက်သေခံလက်မှတ်များကို ငှားရမ်းသုံးစွဲသူများ ဖြစ်ပါသည်။ CA များသည် တစ်ဦးချင်း သော်လည်းကောင်း၊ အဖွဲ့အစည်းသော်လည်းကောင်း ဖြစ်နိုင်ပါသည်။ အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေးဗဟိုအဖွဲ့၏ခွင့်ပြုချက်ဖြင့် ကြီးကြပ်မှုအဖွဲ့မှ ထုတ်ပေးထားသော လိုင်စင်ရရှိထားသော CA များသာ မြန်မာနိုင်ငံအတွင်းတွင် CA အဖြစ်လုပ်ဆောင်နိုင်ပါသည်။

CA များသည် အောက်ပါအခြေအနေများတွင် ကြီးကြပ်မှုအဖွဲ့သို့ ဆက်သွယ်အကြောင်းကြား ရမည်။

- ယင်းတို့၏ CPS နှင့် CP တွင် ပြုပြင်ပြောင်းလဲမှုများပြုလုပ်ခြင်း၊
- ပုံမှန်စာရင်းစစ် အစီရင်ခံစာများ တင်သွင်းခြင်း၊
- ယင်းတို့၏ Private Key များဖောက်ခံရခြင်း (Compromise) ၊
- Technical Audit အစီရင်ခံစာများပေးပို့ခြင်း၊

CA များသည် အောက်ပါအခြေအနေများတွင် Root CA သို့ ဆက်သွယ်အကြောင်းကြားရမည်။

- သက်သေခံလက်မှတ်ငှားရမ်းသုံးစွဲသူများအား သက်သေခံလက်မှတ်ထုတ်ပေးခြင်း၊
- သက်သေခံလက်မှတ်ပယ်ဖျက်စာရင်း (CRL) များထုတ်ပြန်ခြင်း၊
- အကြောင်းကြားစာပေးဖို့သင့်သောကိစ္စရပ်များ၊

၁. ၃. ၅ သက်သေခံလက်မှတ် ငှားရမ်းသုံးစွဲသူများ (Subscriber)

CA များကထုတ်ပေးသော သက်သေခံလက်မှတ်ကို ငှားရမ်းသုံးစွဲသူအား သက်သေခံလက်မှတ် ငှားရမ်းသုံးစွဲသူ (**Subscriber**) များဟု ခေါ်ဆိုပါသည်။

သက်သေခံလက်မှတ် ငှားရမ်းသုံးစွဲသူ (Subscriber)များသည် တစ်ဦးချင်းသော်လည်းကောင်း၊ အဖွဲ့အစည်းသော်လည်းကောင်း ဖြစ်နိုင်ပါသည်။

၁. ၃. ၆ သက်သေခံလက်မှတ်ကို ယုံကြည်စိတ်ချစွာ လက်ခံအသုံးပြုသူများ (Relying Parties)

Root CA မှ ထုတ်ပေးသော သက်သေခံလက်မှတ်များနှင့် ထိုသက်သေခံလက်မှတ်ကို အသုံးပြုပြီး ရေးထိုးထားသော ဒစ်ဂျစ်တယ်လက်မှတ်များကို ယုံကြည်စိတ်ချစွာ လက်ခံသုံးစွဲသော သူများသည် Relying Party များ ဖြစ်ပါသည်။ ထိုသူများမှာ -

၁။ CA များ၊

၂။ CA များ၏ သက်သေခံလက်မှတ်ငှားရမ်းသုံးစွဲသူများ၊

၃။ Root CA နှင့် Cross-Certification ပြုလုပ်ထားသည့် Foreign CA များ၊

၄။ Root CA နှင့် cross- certification ပြုလုပ်ထားသည့် Foreign CA များ၏ သက်သေခံလက်မှတ် ငှားရမ်းသုံးစွဲသူများ၊

၅။ Root CA နှင့် CA များမှ ထုတ်ပေးသောသက်သေခံလက်မှတ်များနှင့် ARL/ CRL များကို လက်ခံအသုံးပြုသူများ၊

သက်သေခံလက်မှတ်ငှားရမ်းသုံးစွဲသူများ(Subscriber) နှင့် သက်သေခံလက်မှတ်ကို ယုံကြည်လက်ခံအသုံးပြုသူ (Relying Parties) များသည် မိမိတို့သုံးစွဲသော သက်သေခံလက်မှတ်သည် CA မှထုတ်ပေးသော သက်သေခံ လက်မှတ်များ ဖြစ်ကြောင်း သေချာစေရမည်။

၁. ၃. ၇ မှတ်ပုံတင်ခွင့် လုပ်ပေးပိုင်ခွင့်ရှိသူ (Registration Authority (RA))

မှတ်ပုံတင်ခွင့်လုပ်ပေးပိုင်ခွင့်ရှိသူ (RA) ဆိုသည်မှာ သက်သေခံလက်မှတ်လျှောက်ထားသူ၏ အကြောင်းအရာများနှင့် ပတ်သက်၍ လက်ခံဆောင်ရွက် မှတ်တမ်းတင်ခြင်း (Registration)၊ လျှောက်ထားသူ အမှန်အကန် ဟုတ်မဟုတ်စစ်ဆေးခြင်း (Identification) နှင့် သက်သေခံမှုစစ်ဆေးခြင်း (Authentication) တို့အတွက် တာဝန်ယူ ဆောင်ရွက်ပေးသော လူပုဂ္ဂိုလ် (သို့မဟုတ်) အဖွဲ့အစည်းတစ်ခု ဖြစ်ပါသည်။ (ဆိုလိုသည်မှာ RA သည် CA ကိုယ်စားမှန်ကန်မှုရှိ၊ မရှိ စစ်ဆေးခြင်း (Identification) နှင့် သက်သေခံမှုစစ်ဆေးခြင်း (Authentication) တာဝန်များကို ဆောင်ရွက်ပေးပါသည်။)

၁. ၃. ၈ အမျိုးသား သက်သေခံလက်မှတ် မှတ်တမ်းတိုက် (National Repository of Digital Certificates)

အမျိုးသားသက်သေခံလက်မှတ်မှတ်တမ်းတိုက်(**National Repository**) ဆိုသည်မှာ Root CA နှင့် CA များမှ ထုတ်ပေးထားသော သက်သေခံလက်မှတ်အားလုံးကို အများပြည်သူ ကြည့်ရှုနိုင်ရန် သိမ်းဆည်း မှတ်တမ်းတင်ထားသည့် သက်သေခံ လက်မှတ် မှတ်တမ်းတိုက်ဖြစ်ပါသည်။

၁. ၃. ၉ CP သင့်တော်အသုံးဝင်မှု (Applicability)

ဤ CP သည် Root CA မှထုတ်ပေးသည့် သက်သေခံလက်မှတ်အားလုံးနှင့် သက်ဆိုင်ပါသည်။ ဤ CP ရှိ လုပ်ထုံးလုပ်နည်းများ၊ လိုက်နာကျင့်သုံးမည့်နည်းလမ်းများ (Practices) အားလုံးသည် မြန်မာနိုင်ငံအတွင်းတွင် Root CA မှ CA များသို့ ထုတ်ပေးထားသည့် သက်သေခံလက်မှတ်၊ သက်သေခံ လက်မှတ် ပယ်ဖျက်စာရင်းများ (Authority Revocation List (ARLs))၊ ဌားရမ်းသုံးစွဲသူများ၏သက်သေခံလက်မှတ်များ၊ သက်သေခံ လက်မှတ် ပယ်ဖျက်စာရင်းများ (CRLs) များကို အသုံးပြုခြင်းများ အားလုံးနှင့် သက်ဆိုင်အကျုံးဝင်ပါသည်။

၁. ၄ သက်သေခံလက်မှတ် အသုံးပြုမှု (Certificate Usage)

၁. ၄. ၁ သက်သေခံလက်မှတ်ကို သင့်တော်သောအသုံးချမှု (Appropriate Certificate Usage)

Root CA မှ CA များအတွက် ထုတ်ပေးသော သက်သေခံလက်မှတ်များကို အောက်ပါအတိုင်း အသုံးပြုရမည်။

- သက်သေခံလက်မှတ် ဌားရမ်းသုံးစွဲသူ (Subscriber)များအား သက်သေခံလက်မှတ် ထုတ်ပေးရန်နှင့်
- သက်သေခံလက်မှတ်ပယ်ဖျက်စာရင်း (Certificate Revocation Lists) များအား လက်မှတ်ရေးထိုးရန် ။

CA များမှ သက်သေခံလက်မှတ်ဌားရမ်းသုံးစွဲသူ (Subscriber) များအား ထုတ်ပေးသော သက်သေခံလက်မှတ်ကို လက်မှတ်ရေးထိုးရန် (Sign) ၊ email ကို လျှို့ဝှက်ကုဒ်ပြောင်း၍ (Encrypt) ပေးပို့နိုင်ရန်၊ မူလစာအတိုင်း ပြောင်းလဲဖတ်ရှုနိုင်ရန် (Decrypt) နှင့် Application များကို Authenticate (Client/ Sever Authentication) ပြုလုပ်ရန်၊ Code Signing ပြုလုပ်ရန် တို့အတွက် အသုံးပြုနိုင်ပါသည်။ Relying party မှ ယုံကြည်စိတ်ချ၍ ယင်းရည်ရွယ်ချက်များအပြင် အခြားသော ရည်ရွယ်ချက်များအတွက် အသုံးပြုလိုပါက အီလက်ထရောနစ်ဆက်သွယ်ဆောင်ရွက်ရေးဥပဒေ၊ နည်းဥပဒေများ၊ ဤ CP၊ CPS တို့နှင့် ကိုက်ညီမှုရှိပြီး၊ သက်သေခံလက်မှတ်ဌားရမ်းသုံးစွဲသူနှင့်လည်း သဘောတူညီချက်ရှိခဲ့လျှင် သက်သေခံလက်မှတ်ကို အသုံးပြုနိုင်ပါသည်။ သက်သေခံလက်မှတ် အမျိုးအစားအားဖြင့် အောက်ပါအတိုင်း သုံးမျိုးရှိပါသည်။

Certificate Class	Assurance Level			Usage		
	Low	Medium	High	Signing	encryption	Client Authentication
Class-1 Certificate	✔			✔	✔	✔
Class-2 Certificate		✔		✔	✔	✔
Class-3 Certificate			✔	✔	✔	✔

Table (1)- Certificate Usage.

Class 1 Certificate

Class 1 အမျိုးအစား သက်သေခံလက်မှတ်သည် လူကိုယ်တိုင်လာရောက် လျှောက်ထားရန်မလိုဘဲ **email** ဖြင့် **online** လျှောက်ထားသူများကို ထုတ်ပေးသော သက်သေခံလက်မှတ်အမျိုးအစား ဖြစ်ပါသည်။

Class 2 Certificate

Class 2 အမျိုးအစား သက်သေခံလက်မှတ်ကို လျှောက်ထားသူမှ လိုအပ်သော အထောက်အထား စာရွက်စာတမ်းများနှင့်တကွ လျှောက်ထားရမည်ဖြစ်ပါသည်။ လိုအပ်သော အထောက်အထားများတွင် အနည်းဆုံးအနေဖြင့် အောက်ပါတို့ပါဝင်ရမည်။

(၁) မှတ်ပုံတင်မူရင်းနှင့် မိတ္တူ၊

(၂) သန်းခေါင်စာရင်း မူရင်းနှင့် မိတ္တူ၊

(၃) ရဲစခန်းထောက်ခံစာ နှင့်

(၄) အဖွဲ့အစည်းများဖြစ်ပါက ကုမ္ပဏီမှတ်ပုံတင်မူရင်းနှင့် မိတ္တူတို့ဖြစ်ပါသည်။

Class 3 Certificate

Class 3 အမျိုးအစား သက်သေခံလက်မှတ်ကို အထက်ဖော်ပြပါ လိုအပ်သော အထောက်အထား စာရွက်စာတမ်းများနှင့် လျှောက်ထားသူကိုယ်တိုင်မှ လာရောက်လျှောက်ထားခြင်း၊ ထုတ်ယူခြင်း ပြုလုပ်ရမည် ဖြစ်ပါသည်။

Root CA မှ **CA** များအတွက် **Class 3** သက်သေခံလက်မှတ် တစ်မျိုးတည်းကိုသာထုတ်ပေးမည်ဖြစ်ပါသည်။

၁. ၄. ၂ တားမြစ်ထားသည့် သက်သေခံလက်မှတ်အသုံးပြုမှုများ (Prohibited Certificate Uses)

အီလက်ထရောနစ်ဆက်သွယ်ဆောင်ရွက်ရေးဥပဒေ၊ ယင်းနှင့်သက်ဆိုင်သည့် နည်းဥပဒေများ နှင့် အမိန့်ကြေငြာစာ များတွင် ခွင့်ပြုထားသည့် အတိုင်းသာ သက်သေခံလက်မှတ်များကို အသုံးပြုရမည်။ လူကို ထိခိုက်ဒါဏ်ရာရစေနိုင်သော၊ သေဆုံးစေနိုင်သော (သို့) သဘာဝပတ်ဝန်းကျင်ကို ထိခိုက်ပျက်စီးစေသည့် စနစ်များ၊ ယင်းစနစ်များ၏ ထိန်းချုပ်မှုကိရိယာများတွင် သက်သေခံလက်မှတ်ကို ထိန်းချုပ်ရန် ရည်ရွယ်ချက်ဖြင့် အသုံးမပြုရပါ။ CA သက်သေခံလက်မှတ်ကို သက်သေခံလက်မှတ်ငှားရမ်းသုံးစွဲသူများ (Subscriber)သို့ သက်သေခံလက်မှတ်ထုတ်ပေးခြင်း CRL Sign ထိုးခြင်း လုပ်ငန်းများမှလွဲ၍ အခြားသောဆောင်ရွက်မှုများ အတွက် အသုံးမပြုရပါ။

၁. ၅ ပေါ်လစီဆိုင်ရာ စီမံအုပ်ချုပ်ရေးရာများ (Policy Administration)

၁. ၅. ၁ CP/CPS အားစီမံအုပ်ချုပ်ရေးဆိုင်ရာ အဖွဲ့အစည်း (Organization Administering the Document)

Address - Myanmar Info-Tech Corporation Ltd.
Universities' Hlaing Campus,
Hlaing Township, Yangon, Myanmar
Attension- Project Department
Phone - 652272, 652273, 652274
Fax - 652275
e-Mail - rootcamm@rootca.org.mm,

၁. ၅. ၂ ဆက်သွယ်ရမည့်သူ (Contact Person)

The Chief Technical Officer
Myanmar Info-Tech Corporation Ltd.
Universities' Hlaing Campus,
Hlaing Township, Yangon, Myanmar
Attension - Project Department
Phone - 652272, 652273, 652274
Fax - 652275
e-Mail - rootcamm@rootca.org.mm,

၁. ၅. ၃ CP/CPS ၏သင့်လျော်မှုကိုဆုံးဖြတ်ပေးမည့်သူ (Person Determining CP/CPS Suitability for the Policy)

ကြီးကြပ်မှုအဖွဲ့ သည် CP/CPS ၏ သင့်လျော်မှုနှင့် အသုံးဝင်မှုကို ဆုံးဖြတ် ပေးပါသည်။

၁. ၅. ၄ CP/CPS ကိုအတည်ပြုပေးသည့်လုပ်ထုံးလုပ်နည်းများ (CP/CPS Approval Procedure)

ဤ CP နှင့် **CPS** ကို ဗဟိုအဖွဲ့၏ သဘောတူညီချက်ဖြင့် ကြီးကြပ်မှုအဖွဲ့မှ အတည်ပြုပြီးဖြစ်ပါသည်။ CP ကို ပြင်ဆင်ချက်များ (amendments) ရှိလျှင် ကြီးကြပ်မှုအဖွဲ့အား တင်ပြအတည်ပြုချက်ရယူပြီး Root CA မှ ပြုလုပ်နိုင်ပါသည်။ ပြင်ဆင်သည့် Versionနှင့် ပြင်ဆင်မှုများ (Updates) ကိုRoot CA ၏ Web Site ရှိ http://www.rootca.org.mm တွင် ဖော်ပြထားပါသည်။ ပြင်ဆင်မှုများသည် ၄င်း CP ၏ နဂိုမူလ Reference version ရှိ ရည်ရွယ်ထားသည့် (designated) (သို့) ဆန့်ကျင်မှုများ (conflicts) ဖြစ်ပေါ်နေသည့်အချက်များကို နေရာယူ/လွှမ်းမိုးမှု (supersede) ရှိပါသည်။ CPS တွင် ပြင်ဆင်မှုကြောင့် CP တွင် ပြင်ဆင်ရန်လိုအပ်ပါက ကြီးကြပ်မှု အဖွဲ့ထံတင်ပြပြီးခွင့်ပြုချက်ဖြင့် ဆောင်ရွက်ပါသည်။

၁. ၆ အဓိပ္ပါယ်သတ်မှတ်ချက်နှင့်အတိုကောက်စာလုံးများ (Definitions and Acronyms)

နောက်ဆက်တွဲ(က) နှင့် နောက်ဆက်တွဲ(ခ) ဇယားတွင် ဖော်ပြထားပါသည်။

၂. ပုံနှိပ်ထုတ်ဝေခြင်းနှင့် အမျိုးသား သက်သေခံလက်မှတ် မှတ်တမ်းတိုက်၏ တာဝန်များ (Publication and National Repository Responsibilities)

၂. ၁ အမျိုးသားသက်သေခံလက်မှတ် မှတ်တမ်းတိုက် (National Repository)

Root CA သည် Online အမျိုးသားသက်သေခံလက်မှတ် မှတ်တမ်းတိုက် (National Repository) ထားရှိရမည်ဖြစ်ပြီး Root CA လက်အောက်ရှိ CA များမှလည်း မိမိတို့ ၏ သက်သေခံလက်မှတ်မှတ်တမ်းတိုက် (Repository) များထားရှိရမည်ဖြစ်သည်။ Root CA မှ ထုတ်ပေးသော သက်သေခံလက်မှတ်များနှင့် သက်သေခံလက်မှတ်ပယ်ဖျက်စာရင်း(ARL)များ၊ ယင်းလက်အောက်ရှိ CA များမှ ထုတ်ပေးသော သက်သေခံလက်မှတ်များနှင့် ဖျက်သိမ်းထားသော လက်မှတ်များ(CRL) များကို အမျိုးသားသက်သေခံလက်မှတ် မှတ်တမ်းတိုက်တွင် အများပြည်သူ ကြည့်ရှုနိုင်ရန်အလို့ငှာ ထုတ်ဝေဖော်ပြ ပေးထားမည်ဖြစ်ပါသည်။ ယင်းအပြင် သက်သေခံ လက်မှတ်ကို ယုံကြည်စွာလက်ခံ အသုံးပြုသူများ (Relying Party) များမှ သက်သေခံလက်မှတ်၏ အခြေအနေ (Certificate Status) နှင့်ပါတ်သက်သော အချက်အလက်များကို သင့်လျော်သော Repository နှင့် LDAP တို့မှ ရှာဖွေနိုင်ရန် သတင်းအချက်အလက်များကိုလည်း ပေးထားရမည်။ OCSP (Online Certificate

Status Protocol) ရှိပါက သင့်လျော်သော၊ မှန်ကန်သော OCSP Responder ကိုရှာဖွေနိုင်ရန်လည်း ထိုအချက်အလက် များကို ဖော်ပြပေးထားပါမည်။

၂.၂ သက်သေခံလက်မှတ်အချက်အလက်များကို ပုံနှိပ်ထုတ်ဝေခြင်း (Publication of Certificate Information)

Root CA သည် သက်သေခံလက်မှတ်ကိုယုံကြည်စွာလက်ခံအသုံးပြုသူ (Relying Parties) များမှ သက်သေခံလက်မှတ်၏အခြေအနေ(Status) နှင့် Root CA မှ ထုတ်ပေးထားသောသက်သေခံလက်မှတ် ပယ်ဖျက်စာရင်းများ (ARL)၊ CA မှ ထုတ်ပေးထားသောသက်သေခံလက်မှတ် ပယ်ဖျက်စာရင်းများ (CRL)နှင့် ပါတ်သက်သည့် စုံစမ်းမှုများ ပြုလုပ်နိုင်ရန်၊ Certificateများ၊ ပယ်ဖျက်စာရင်းများကို Download ပြုလုပ်နိုင်ရန် အမျိုးသားသက်သေခံလက်မှတ် မှတ်တမ်းတိုက် (National Repository) ထားရှိပါသည်။ ထို့အပြင် OCSP စံနစ်ရှိပါက Relying Partyများမှ သက်သေခံလက်မှတ်အား စစ်ဆေးနိုင်မည့်နည်းလမ်းများကို ဖော်ပြ ပေးထားပါမည်။

Root CA သည် အောက်ပါအချက်အလက်များကို မည်သူမဆိုကြည့်ရှုနိုင်ရန် ထုတ်ပြန် (Publish) ထားပါသည်။ Root CA ၏ Web site http://www.rootca.org.mm တွင် အချိန်ပြည့် (Internet ဆက်သွယ်မှု ပြတ်တောက်နေချိန် သို့မဟုတ် စနစ်ပြုပြင်ထိန်းသိမ်းရေး (System Maintenance) ပြုလုပ်နေသဖြင့် ယာယီ ရပ်ဆိုင်းထားချိန်တို့မှလွဲ၍) ဖော်ပြထားပါသည်။

Root CA မှ ထုတ်ပြန်ထားသည်များမှာ အောက်ပါအတိုင်းဖြစ်ပါသည်။

၁။ Root CA ၏ Certification Practice Statement (CPS) ၊

၂။ Root CA ၏ Certificate Policy (CP) ၊

၃။ Root CA ၏သက်သေခံလက်မှတ်၊

၄။ Root CA ၏ နောက်ဆုံးထုတ်ပြန်ထားသော ARL များ ၊

၅။ CA များ၏သက်သေခံလက်မှတ်များ၊

၆။ CAများမှထုတ်ပေးသည့်သက်သေခံလက်မှတ်များနှင့် သက်သေခံလက်မှတ် ပယ်ဖျက် စာရင်းများ ၊

၇။ Relying Party Agreements

၂.၃ ပုံနှိပ်ထုတ်ဝေမည့်အကြိမ်နှင့်အချိန် (Time or Frequency of Publication)

Root CA ၏ သက်သေခံလက်မှတ်ပယ်ဖျက်စာရင်း(ARL) များကို CA တစ်ခုမှ သက်သေခံလက်မှတ်ဖျက်သိမ်းသည့်အခါတိုင်း ထုတ်ပြန်ပေးမည်။ အကယ်၍ ARL တွင်ဖော်ပြထားသော

သက်သေခံလက်မှတ်မှာ သက်တမ်းကုန်ဆုံးသွားပါက ထိုသက်သေခံလက်မှတ် သက်တမ်းကုန်ဆုံးပြီးနောက်ပိုင်း ထုတ်ပြန်ထားသော ARL များတွင် ယင်းကို ထည့်သွင်းလိမ့်မည် မဟုတ်ပါ။

၂.၄ အမျိုးသားသက်သေခံလက်မှတ် မှတ်တမ်းတိုက်ရှိ အချက်အလက်များထိန်းချုပ်မှု (Access Controls on National Respository)

Root CA သည် အမျိုးသားသက်သေခံလက်မှတ် မှတ်တမ်းတိုက်ရှိ အချက်အလက်(Data) များအား လုပ်ပိုင်ခွင့်မရှိသော ပုဂ္ဂိုလ်များမှ ထပ်မံဖြည့်စွက်ခြင်း၊ ဖျက်ခြင်း၊ ပြုပြင်ခြင်းများမပြုလုပ်နိုင်ရန် လိုအပ်သော ကာကွယ်ထိန်းချုပ်မှု အစီအမံ (Control) များ ပြုလုပ်ထားပါသည်။ အမျိုးသားသက်သေခံလက်မှတ် မှတ်တမ်းတိုက်အား ဝင်ရောက်ကြည့်ရှုခြင်းကို ကန့်သတ်ထားခြင်းမရှိပါ။ သို့သော် အမျိုးသားသက်သေခံလက်မှတ် မှတ်တမ်းတိုက်အား ဝင်ရောက်ကြည့်ရှုအသုံးပြုသူများသည် Root CA ၏ Relying Party Agreements (သို့) CRL Usage Agreements များ(ရှိပါက) ကို သဘောတူညီမှုရှိမှသာ ဝင်ရောက်ကြည့်ရှုခြင်း၊ အသုံးပြုခြင်း ပြုလုပ်နိုင်ပါသည်။

၃. သက်သေခံခြင်းနှင့်စစ်ဆေးခြင်း (Identification and Authentication)

၃.၁ အမည်ပေးခြင်း (Naming)

Root CA သည် သက်သေခံလက်မှတ် တွင် ဖော်ပြထားသော အမည် များအား စစ်မှန်မှုစစ်ဆေးခြင်း (Authentication) ပြုလုပ်ပါသည်။

၃.၁.၁ အမည်အမျိုးအစားများ (Type of Names)

Root CA မှ ထုတ်ပေးသော သက်သေခံလက်မှတ်ရှိ Subject Name Field ၏ X. 501 Distinguished Name (DN) ပါရှိပါသည်။

CA အဖွဲ့အစည်းသက်သေခံလက်မှတ်များ၏ Subject Distinguished Name တွင် Domain Name ၊ အဖွဲ့အစည်း၏ e-mail လိပ်စာ၊ အဖွဲ့အစည်း၏တရားဝင်အမည် (သို့) အဖွဲ့အစည်း၏ Private Key ကို အသုံးပြုမည့် Authorized Representative ၏အမည် ပါရှိပါသည်။

သက်သေခံလက်မှတ်များ၏ Organization (O=) အမည်တွင် အဖွဲ့အစည်း၏ တရားဝင်အမည် ဖြစ်ရပါမည်။

တစ်ဦးတစ်ယောက်ချင်းအတွက် ထုတ်ပေးသော သက်သေခံလက်မှတ်၏ Common Name တွင် ရှိသောအမည်သည် ထိုသူ၏ အများမှ လက်ခံသော Personnel Name ဖြစ်ရမည်။

၃. ၁. ၂ အမည်များ အဓိပ္ပါယ်ရှင်းလင်းလွယ်ကူရန်လိုအပ်ခြင်း (Need for Name to be Meaningful)

CA များနှင့် ယင်း၏ သက်သေခံလက်မှတ်ဌာနရမ်းသုံးစွဲသူများသည်သက်သေခံလက်မှတ်များ ၏ Subject Field တွင်ပါဝင်မည့်အမည်များကို CA ၏တည်ရှိမှုကို ဆုံးဖြတ်ချက်ပေးနိုင်သော၊ နားလည်ရန် လွယ်ကူသည့်၊ အများသိရှိသော ရှင်းလင်း ၊ အဓိပ္ပါယ်ရှိသည့် အမည်များကို အသုံးပြုရမည်။

၃. ၁. ၃ သက်သေခံလက်မှတ်ဌာနရမ်းသုံးစွဲသူ၏ အမည်ကွဲများ (Anonymity or Pseudonymity of CAs)

Root CA သည် သက်သေခံလက်မှတ်လျှောက်ထားသူ(CA)များအား မိမိ (သို့) အဖွဲ့အစည်း ၏ အမည်များကို နာမည်ရင်း မဟုတ်သည့် အခြားသောအမည်များ ထားရှိသုံးစွဲခွင့် မပြုပါ။

၃. ၁. ၄ အမည်များကို အဓိပ္ပါယ်ကောက်ယူမည့် စည်းမျဉ်းများ (Rules for Interpreting Various Name Forms)

လိုအပ်သလို ပြဋ္ဌာန်းပါသည်။

၃. ၁. ၅ အမည်များထပ်တူမှုမရှိခြင်း (Uniqueness of Names)

သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူအဖြစ်လျှောက်ထားသူ(CA)များ၏ Subject Distinguished Name များသည် Root CA နှင့် သီးခြား CA တစ်ခု၏ Domain အတွင်းတွင် အမည် ထပ်တူခြင်းမရှိရ။

၃. ၁. ၆ အသိအမှတ်ပြုခြင်း၊ စစ်မှန်ကြောင်းထင်ရှားစေခြင်းနှင့် ကုန်ပစ္စည်းအမှတ်အသားများ၏ အခန်းကဏ္ဍ

(Recognition, Authentication and Role of Trademarks)

Root CA သည် သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူအဖြစ်လျှောက်ထားသူများကို သက်သေခံလက်မှတ် လျှောက်ထားခြင်းပြုသည့်အခါတွင် အခြားသူများ၏ ဉာဏ်စွမ်းရည်ပိုင်ဆိုင်မှုဆိုင်ရာ အခွင့်အရေး (Intellectual Property Right (IPR)) ကိုကျူးလွန်မှုဖြစ်စေသည့် အမည်များသုံးစွဲ လျှောက်ထားခြင်း ခွင့်မပြုပါ။ လျှောက်ထားသူများသည် အခြားသူ များ၏ IPR ကို ဖောက်ဖျက်ခြင်းရှိမရှိကို Root CA မှ စစ်ဆေးခြင်းမပြုလုပ်ပါ။ အကယ်၍ ထိုသို့ အငြင်းပွားမှုများ ပေါ်ပေါက်လာပါက Root CA သည် ထိုသူ၏ သက်သေခံလက်မှတ်ကို ကြီးကြပ်မှု အဖွဲ့၏ ခွင့်ပြုချက်ဖြင့် ပယ်ဖျက်ခြင်း၊ ဆိုင်းငံ့ခြင်းပြုလုပ်ရာတွင် လျော်ကြေးပေးရန် မလိုအပ်ပါ။

၃. ၂ ကနဦး မည်သူမည်ဝါဖြစ်ကြောင်း စစ်ဆေးခြင်း (Initial Identity Validation)

၃. ၂. ၁ Private Key ပိုင်ဆိုင်ကြောင်းသက်သေပြမည့်နည်းလမ်း (Method to prove possession of Private Key)

CA သည် သက်သေခံလက်မှတ်ထုတ်ရာတွင်အသုံးပြုမည့် Private Key သည် ၎င်းပိုင်ဆိုင်မှု မှန်ကန်ကြောင်း သက်သေပြနိုင်ရမည်။ ထိုသို့သက်သေပြရာတွင် PKCS#10 File (သို့) အခြားသော Cyrptographic နည်းလမ်းများ (သို့) Root CA မှသဘောတူထားသည့်နည်းလမ်းများဖြင့် သက်သေပြနိုင်ပါသည်။ သက်သေခံ လက်မှတ်လျှောက်ထားသူ CA ကိုယ်စား Root CA မှ Key Pair ထုတ်ခြင်းဆောင်ရွက်ပေးပါက Private Key ပိုင်ဆိုင်ကြောင်း သက်သေပြရန် မလိုအပ်ပါ။

၃. ၂. ၂ အဖွဲ့အစည်း စစ်မှန်မှုရှိကြောင်း ထင်ရှားစေရန် စစ်ဆေးခြင်း (Authentication of Organization Identity)

သက်သေခံလက်မှတ်တွင် အဖွဲ့အစည်းအမည်များပါဝင်သည့်အခါတိုင်းတွင် ထိုအဖွဲ့အစည်း အမှန်တကယ် တည်ရှိမှုနှင့် သက်သေခံလက်မှတ်လျှောက်ထားသူမှပေးသော အခြားလျှောက်ထားမှုပါအချက်များ (စစ်ဆေးရန် မလိုအပ်သည့် အချက်များမှ လွဲ၍) မှန်ကန်မှုရှိကြောင်းကို စစ်ဆေးပြီးမှ ကြီးကြပ်မှု အဖွဲ့၏ တာဝန်ပေးအပ်ချက် အတိုင်း Root CA မှ သက်သေခံလက်မှတ်ထုတ်ပေးခြင်းကို ဆောင်ရွက်ပါသည်။

သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ(CA) လျှောက်ထားသူအား စစ်ဆေးရာတွင် အနိမ့်ဆုံးအဆင့် အားဖြင့်-

- အဖွဲ့အစည်းအမှန်တကယ်တည်ရှိကြောင်းကို အစိုးရအဖွဲ့အစည်းမှ ထုတ်ပေးထားသည့် အဖွဲ့အစည်း ဆိုင်ရာ စာရွက်စာတမ်းများ (သို့) အဖွဲ့အစည်းတည်ရှိမှုကို အာမခံနိုင်သည့် အာဏာပိုင်အဖွဲ့အစည်း တစ်ခုခု၏ စာရွက်စာတမ်း၊ ထောက်ခံချက်များကို စစ်ဆေးခြင်းများပြုလုပ်ပါမည်။
- သက်သေခံလက်မှတ်လျှောက်ထားသူအား ယင်းအဖွဲ့အစည်းမှ ခွင့်ပြုချက်ဖြင့် လျှောက်ထားခြင်း ဖြစ်ကြောင်း၊ အဖွဲ့အစည်းမှ သိရှိကြောင်းကို တယ်လီဖုန်း (သို့) စာ (သို့) အခြားသောနည်းလမ်းများကို သုံး၍ စစ်ဆေးအတည်ပြုပါသည်။ သက်သေခံလက်မှတ်တွင် ပုဂ္ဂိုလ် တစ်ဦးဦး၏ အမည်သည် အဖွဲ့အစည်း၏ ကိုယ်စားလှယ် အနေဖြင့် ပါဝင်သည့်အခါ ထိုသူသည် ယင်းအဖွဲ့အစည်း၏ ဝန်ထမ်း ဟုတ်/မဟုတ် ၊ အဖွဲ့အစည်းကိုယ်စား လုပ်ပိုင်ခွင့် ရှိ/မရှိကို ကြီးကြပ်မှု အဖွဲ့မှ စစ်ဆေးပါမည်။ သက်သေခံလက်မှတ်တွင် Domain name (သို့) e-mail Domain များပါဝင်ပါက သက်သေခံလက်မှတ် လျှောက်ထားသူသည် ထို Domain name ကိုသုံးစွဲခွင့် နှင့် e-mail domain name ကို သုံးစွဲခွင့်ရှိ/မရှိတို့ကို စစ်ဆေး မည် ဖြစ်ပါသည်။

- အစိုးရအဖွဲ့အစည်းများ၊ ဗဟိုအဖွဲ့နှင့် ကြီးကြပ်မှုအဖွဲ့တို့မှ သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ (CA) လုပ်ငန်းဆောင်ရွက်ရန် တိုက်ရိုက်တာဝန်ပေးအပ်ထားသည့် လူပုဂ္ဂိုလ်အဖွဲ့အစည်းများအတွက် အထက်ပါ အတည်ပြုစစ်ဆေးခြင်းများ ပြုလုပ်ရန် မလိုအပ်ပါ။

မြန်မာနိုင်ငံအစိုးရမှ ပြဋ္ဌာန်းထားသော ဥပဒေများ၊ သက်ဆိုင်သည့်နည်းဥပဒေများ၊ အမိန့်ကြော်ငြာစာများ၊ လိုင်စင်စာရွက်စာတမ်းများနှင့် လုပ်ထုံးလုပ်နည်းများအတိုင်း အခြားသော စစ်ဆေးမှုများကို လိုအပ်ပါက ပြုလုပ်သွားမည် ဖြစ်ပါသည်။

၃. ၂. ၃ တစ်ဦးချင်းစီ၏ တည်ရှိမှုကို စစ်ဆေးခြင်း (Authentication of Identity)

Root CA သည် သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူအဖြစ် လိုင်စင်ခွင့်ပြုထားသောသူအား ထိုသူအစစ်အမှန် ဟုတ်မဟုတ်ကို လိုင်စင်ပါ အချက်အလက်များနှင့် ပူးတွဲပါ စာရွက်စာတမ်းများနှင့် တိုက်ဆိုင်စစ်ဆေးခြင်းများပြုလုပ်ပါသည်။

၃. ၂. ၄ အချင်းချင်းလုပ်ငန်းလုပ်ဆောင်နိုင်မှုရှိရန်အတွက် သက်မှတ်ချက်များ (Criteria For Interoperation)

လိုအပ်သလို ပြဋ္ဌာန်းပါသည်။

၃. ၃ သက်တမ်းတိုးရန်လျှောက်ထားမှုများကို မှန်ကန်မှုရှိမရှိ စစ်ဆေးခြင်းနှင့် သက်သေခံမှု စစ်ဆေးခြင်း (Identification and Authentication for Re-key Request)

CA များ၏ သက်သေခံလက်မှတ်များ သက်တမ်းမကုန်ဆုံးမီ သက်သေခံလက်မှတ် အသုံးပြုခြင်း ပြတ်တောက်သွားခြင်း မရှိစေရန်အတွက် သက်သေခံလက်မှတ် အသစ်တစ်ခုရရှိရန် လိုအပ်ပါသည်။ Root CA သည် **CA** များမှ သက်သေခံလက်မှတ် သက်တမ်းတိုးတိုင်း အပိုဒ်(၄. ၂)အတိုင်းစစ်ဆေး၍ သက်တမ်းကုန်ဆုံးမည့် သက်သေခံလက်မှတ် နေရာတွင် အစားထိုးရန် သက်သေခံလက်မှတ်အသစ် တစ်ခု ထုတ်ပေးပါသည်။

၃. ၃. ၁ သက်သေခံလက်မှတ် သက်တမ်းတိုးခြင်း (Re-key)ကိစ္စများကို စစ်မှန်ကြောင်းစစ်ဆေးခြင်းနှင့် မှန်ကန်ကြောင်း အတည်ပြု ခြင်း (Identification and Authentication for Routine Re-key)

သက်သေခံလက်မှတ်ကို သက်တမ်းတိုးခြင်း (Re-key) မပြုလုပ်ခင် Re-key လျှောက်ထားခြင်း ပြုလုပ်သူ(လူပုဂ္ဂိုလ်(သို့)အဖွဲ့အစည်း)သည် ထိုသက်သေခံလက်မှတ်ကိုင်ဆောင်သူ CA အစစ်အမှန် ဖြစ်ကြောင်း အပိုဒ်(၄. ၆) ပါ သတ်မှတ်ချက်များအတိုင်းစစ်ဆေးပါသည်။

သက်တမ်းတိုးလျှောက်ရာတွင် ဖြည့်သွင်းသည့်အချက်များနှင့် ကနဦး သက်သေခံလက်မှတ် လျှောက်ထားရာတွင် ဖြည့်သွင်းသည့် အချက်အလက်များ (ကော်ပိုရိတ်နှင့် Technical Contact Information

များအပါအဝင်) ကွဲပြားမှု၊ ပြောင်းလဲမှု မရှိပါက သက်တမ်းတိုးသက်သေခံလက်မှတ်အသစ်ကို ထုတ်ပေးမည် ဖြစ်ပါသည်။ Rekey (သို့) Renewal ပြုလုပ်ရန် တောင်းဆိုသည့် အခါတိုင်းကြီးကြပ်မှုအဖွဲ့သည် သက်သေခံ လက်မှတ် ထုတ်ပေးပိုင်ခွင့်ရှိသူ လိုင်စင်လျှောက်ထားစဉ်က အသုံးပြုသည့် စစ်ဆေးသည့် နည်းလမ်းများ၊ သက်သေခံမူစစ်ဆေးခြင်း ပြုလုပ်သည့်နည်းများအတိုင်း ပြန်လည် စစ်ဆေးပါသည်။

၃. ၃. ၂ သက်သေခံလက်မှတ်ပယ်ဖျက်ပြီးနောက် သက်တမ်းတိုး (Re-Key) ပြုလုပ်ရန် လျှောက်ထားခြင်း များကို စစ်မှန်ကြောင်း စစ်ဆေးခြင်းနှင့် မှန်ကန်ကြောင်း အတည်ပြုခြင်း (Identification and Authentication for Re-key After Revocation)

Root CA သည်အောက်ဖော်ပြပါ အကြောင်းများကြောင့် သက်သေခံလက်မှတ်ကို ပယ်ဖျက်ခံရပြီးနောက် သက်တမ်းတိုး (Re-key နှင့် Renewal) ပြုလုပ်ရန် လျှောက်ထားလာခြင်းများကို ခွင့်ပြုမည်မဟုတ်ပါ။

၁။ သက်သေခံလက်မှတ်ပါအချက်များသည် မှားယွင်းဖော်ပြထားကြောင်း သိရှိ၍ ပယ်ဖျက်ခြင်းခံ ရလျှင်၊

၂။ သက်သေခံလက်မှတ်လျှောက်ထားစဉ်က အချက်များ မှားယွင်းဖော်ပြထား၍ သက်သေခံ လက်မှတ်ပယ်ဖျက်ခြင်းခံရလျှင်၊

၃။ ကြီးကြပ်မှုအဖွဲ့မှ ညွှန်ကြားချက်ဖြင့် ပယ်ဖျက်ခြင်းခံရလျှင်၊

၃. ၄ CA ၏ သက်သေခံလက်မှတ်ပယ်ဖျက်ရန် တောင်းဆိုခြင်းအတွက် စစ်မှန်ကြောင်းစစ်ဆေးခြင်းနှင့် မှန်ကန်ကြောင်း အတည်ပြုခြင်း၊ (Identification and Authentication for Revocation Request)

Root CA သည် **CA** များ၏ သက်သေခံလက်မှတ်အား ကြီးကြပ်မှု အဖွဲ့၏ ခွင့်ပြုချက်ဖြင့်သာ ပယ်ဖျက်ပါသည်။ သက်သေခံလက်မှတ် ပယ်ဖျက်ရန် **Root CA** နှင့် CA ကိုယ်တိုင်မှ တောင်းဆို လျှောက်ထား ခြင်းများကို ပယ်ဖျက်ခြင်းမပြုမီ ကြီးကြပ်မှုအဖွဲ့မှ သေချာစွာ စစ်ဆေး၍ ဆုံးဖြတ်ပေးမည် ဖြစ်ပါသည်။ သက်သေခံလက်မှတ်အား ပယ်ဖျက်ရန် သက်သေခံလက်မှတ်လျှောက်ထားသူကိုယ်တိုင်မှ တောင်းဆိုရမည်။ **Root CA** သည် **CA** ၏ **Challenge Phrase** ကို အသုံးပြု စစ်မှန်ကြောင်း စစ်ဆေးခြင်း ပြုလုပ်ပါသည်။

၄. သက်သေခံလက်မှတ် Life-Cycle လုပ်ငန်းဆောင်ရွက်မှု လိုအပ်ချက်များ (Certificate Life-Cycle Operational Requirements)

၄. ၁ သက်သေခံလက်မှတ် လျှောက်ထားခြင်း (Certificate Application)

သက်သေခံလက်မှတ် ထုတ်ပေးပိုင်ခွင့်ရှိသူ (CA) အဖြစ် လျှောက်ထားခြင်းလျှောက်လွှာကို ဖြည့်စွက်၍ အောက်ဖော်ပြပါ ရုံးသို့လူကိုယ်တိုင်လာရောက် လျှောက်ထားရမည်။

အတွင်းရေးမှူး
အီလက်ထရောနစ်ဆက်သွယ်ဆောင်ရွက်ရေး ကြီးကြပ်မှုအဖွဲ့
ရုံးအမှတ် (၂) ၊ အထူးဖွံ့ဖြိုးရေးဇုန်၊
ဆက်သွယ်ရေးစာတိုက်နှင့် ကြေးနန်းဝန်ကြီးဌာန၊
နေပြည်တော် ။

၄. ၁. ၁ သက်သေခံလက်မှတ်လျှောက်ထားခွင့်ရှိသူများ (Who Can Submit a Certificate Application?)

ကြီးကြပ်မှုအဖွဲ့မှ ထုတ်ပြန်သည့် ××××××× နေ့ ရက်စွဲပါ အမိန့်ကြော်ငြာစာအမှတ် ---------- ရှိ ဖော်ပြပါ အချက်အလက်များနှင့် ကိုက်ညီသော မည်သူမဆို CA အဖြစ်လုပ်ငန်းလုပ်ဆောင်ခွင့် လျှောက်ထားနိုင်ပါသည်။

၄. ၁. ၂ စာရင်းပေးသွင်းခြင်းလုပ်ငန်းနှင့် လုပ်ငန်းတာဝန်ယူမှုများ (Enrollment Process and Responsibilities)

သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ လိုင်စင်လျှောက်ထားသူ အားလုံးသည် လိုင်စင် လျှောက်ထားခြင်း၊ သက်သေခံလက်မှတ် လျှောက်ထားခြင်းပြုလုပ်ရာတွင် မှန်ကန်သော၊ စစ်မှန်သော အချက် အလက်များကို ဖြည့်စွက်ပေးရမည်။ သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ (CA) သည် Root CA နှင့် လက်မှတ်ရေးထိုးထားသော ဌားရမ်းသုံးစွဲသူသဘောတူညီချက် (Service User Agreement) တွင် ပါဝင်သော အချက်များအတိုင်းဆောင်ရွက် ရမည်။ CA များသည် လိုင်စင်ပါ စည်းကမ်းချက်များ၊ အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေးဥပဒေနှင့်နည်းဥပဒေများ၊အမိန့်ကြေငြာစာများ နှင့် ညွှန်ကြားချက်များကို လိုက်နာရမည်။ လိုင်စင်လျှောက်ထားစဉ်က လက်မှတ်ရေးထိုးသူမှ သက်သေခံလက်မှတ်လျှောက်လွှာတွင် လက်မှတ်ရေးထိုး လျှောက်ထားရမည်။ လျှောက်ထားသူမှ Key Pair (Public Key နှင့် Private Key) ကို မိမိကိုယ်တိုင်ပြုလုပ်ပါက အောက်ပါအတိုင်း ဆောင်ရွက်ရမည်။

(က) Root CA နှင့် ကြီးကြပ်မှုအဖွဲ့ထံသို့ Public Key နှင့်ကိုက်ညီမှုရှိသော Private Key အမှန်တကယ် ပိုင်ဆိုင်ကြောင်း သက်သေပြနိုင်ရန် စီစဉ်ထားရှိခြင်း၊

(ခ) Root CA ထံသို့ ၄င်းတို့၏ Certificate Signing Request File (PKCS #10) ပေးပို့ခြင်း၊ တို့ကို လုပ်ဆောင်ရမည်။

လိုင်စင်လျှောက်ထားသူကိုယ်စား လိုအပ်ပါက Root CA မှ Key Pair Generate ပြုလုပ်ပေးခြင်းကို ဆောင်ရွက်ပေးပါသည်။

၄. ၂ သက်သေခံလက်မှတ်လျှောက်ထားခြင်းကိုလက်ခံဆောင်ရွက်ခြင်း (Certificate Application Processing)

၄. ၂. ၁ စစ်ဆေးခြင်းလုပ်ငန်းများကိုဆောင်ရွက်ခြင်း (Performing Identification and Authentication Functions)

Root CA သည် CA အဖြစ်လျှောက်ထားသူအား သက်သေခံလက်မှတ်ထုတ်ပေးခြင်းမပြုမီ အချက်အလက်များအား စစ်ဆေးခြင်းကို အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေး ဥပဒေ၊ ၄င်းနှင့် သက်ဆိုင်သော နည်းဥပဒေ၊ အမိန့်ကြေငြာစာများတွင် ဖော်ပြထားသည့်အတိုင်း စစ်ဆေးခြင်းကို ဆောင်ရွက် သွားမည် ဖြစ်ပါသည်။ ထို့အပြင် ကြီးကြပ်မှုအဖွဲ့မှ CA လျှောက်ထားသူအား လိုင်စင် ထုတ်ပေးထားခြင်းရှိ၊ မရှိ ၊ လိုင်စင်ပါအချက်များနှင့် သက်သေခံလျှောက်ထားစဉ်က ဖြည့်သွင်းခဲ့သော အချက်အလက်များကို တိုက်ဆိုင် စစ်ဆေးပါသည်။

၄. ၂. ၂ သက်သေခံလက်မှတ်လျှောက်ထားခြင်းကို လက်ခံခြင်း(သို့) ငြင်းပယ်ခြင်း (Approval or Rejection of Certificate Applications)

Root CA သည် သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ (CA) လိုင်စင် ရရှိထားသူများကိုသာ သက်သေခံလက်မှတ်ထုတ်ပေးမည်ဖြစ်ပါသည်။

Root CA သည် အောက်ဖော်ပြပါအချက်များ ဖြစ်ပွားလျှင် သက်သေခံလက်မှတ်ထုတ်ပေးခြင်းကို ငြင်းပယ်နိုင်ရန် ကြီးကြပ်မှုအဖွဲ့သို့ တင်ပြရမည် ဖြစ်ပါသည်။

- အကြောင်းကြားစာကို သတ်မှတ်အချိန်အတွင်း အရေးယူဆောင်ရွက်ခြင်း၊ အကြောင်းပြန်ကြားခြင်းနှင့် CA မှ ဖြည့်ဆည်းဆောင်ရွက်ရမည့် ကိစ္စရပ်များအတွက်ဆောင်ရွက်ခြင်း မရှိခဲ့လျှင်၊
- Root CA သို့ ပေးဆောင်ရမည့် သတ်မှတ်ထားသော ငွေကြေးကိုပေးသွင်းရန် ပျက်ကွက်ခဲ့လျှင်၊
- သက်သေခံ လက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူလျှောက်ထားသူအား သက်သေခံလက်မှတ် ထုတ်ပေးခြင်း သည် Root CA အတွက် နည်းပညာပိုင်းဆိုင်ရာ ထိခိုက်မှုများရှိလာနိုင်လျှင် (သို့မဟုတ်) ရှိလာနိုင်သည် ဟု ယူဆလျှင်၊
- Service User Agreement ကို လက်မှတ်ရေးထိုးခြင်း မပြုလုပ်ခဲ့လျှင်

၄. ၂. ၃ သက်သေခံလက်မှတ်လျှောက်ထားခြင်းကို လက်ခံဆောင်ရွက်ပေးသည့်ကြာမြင့်ချိန် (Time to Process Certificate Applications)

CAလိုင်စင်ရရှိထားသူများမှ သက်သေခံလက်မှတ် လျှောက်လွှာကို ပြည့်စုံအောင်ဖြည့်စွက်ပြီးပါက Root CA သည် (၃)ရက် အတွင်း သက်သေခံလက်မှတ်ကို ထုတ်ပေးမည်ဖြစ် ပါသည်။ Root CA သည် လက်မှတ်ရေးထိုးခြင်းလုပ်ငန်း(signing operations) များကို အစိုးရ ရုံးဖွင့်ရက်များတွင်သာ ပြုလုပ်ပါမည်။

၄. ၃ သက်သေခံလက်မှတ် ထုတ်ပေးခြင်း (Certificate Issuance)

၄. ၃. ၁ Root CA Actions during Certificate Issuance

ကြီးကြပ်မှုအဖွဲ့သည် လိုင်စင်လျှောက်ထားသူ၊ အဖွဲ့အစည်း၏ လုပ်ငန်းဆောင်ရွက်နိုင်မှု အရည်အချင်း၊ ကျွမ်းကျင်မှု၊ ဝန်ထမ်းအင်အား၊ လုပ်ငန်းဆိုင်ရာ အခြေခံအဆောက်အအုံနှင့် လိုအပ်သော အထောက်အပံ့ ပစ္စည်းများ ပြည့်စုံမှု၊ ငွေကြေးတောင့်တင်းမှု၊ ဥပဒေနှင့် လုပ်ထုံးလုပ်နည်းဆိုင်ရာ လိုအပ်ချက်များအပေါ်တွင် အခြေခံ၍ CA အဖြစ်လုပ်ငန်းဆောင်ရွက်မှုလိုင်စင် ထုတ်ပေးမှုကို စာရင်းစစ်ခြင်း ပြုလုပ်၍ စဉ်းစားဆုံးဖြတ်ပါမည်။ Root CA သည် ကြီးကြပ်မှုအဖွဲ့၏ တာဝန်ပေးချက်အရ နည်းပညာဆိုင်ရာ စာရင်းစစ်ခြင်းကို ဆောင်ရွက်ပါသည်။ ထိုစာရင်းစစ်ခြင်းများကို အောင်မြင်ပါက ကြီးကြပ်မှုအဖွဲ့သည် ခွင့်ပြုကြောင်း အကြောင်းကြားစာနှင့်အတူ လျှောက်လွှာမိတ္တူ နှင့် ခွင့်ပြုလိုင်စင်စာရွက် (Paper Licence) မိတ္တူကို Root CA ထံသို့ ပေးပို့ပါသည်။

Root CA သည် CA အား အပိုဒ် (၄. ၂) အတိုင်း စစ်ဆေးမှုများပြုလုပ်၍ မှန်ကန်ပါက သက်သေခံလက်မှတ်ကို ထုတ်ပေးပါသည်။ ထို့နောက် သက်သေခံလက်မှတ် လာရောက်ထုတ်ယူနိုင်ကြောင်းကို လျှောက်ထားသူထံသို့ အကြောင်းကြားစာ ပေးပို့မည် ဖြစ်ပါသည်။ လျှောက်ထားသူမှ ထိုအကြောင်းကြားစာနှင့် အတူ သက်သေခံလက်မှတ်လျှောက်ထားစဉ်က လက်မှတ်ရေးထိုးသူကိုယ်တိုင် Root CA ထံ လာရောက် ထုတ်ယူရမည် ဖြစ်ပါသည်။

၄. ၃. ၂ စာရွက်အထောက်အထားလက်မှတ်ထုတ်ပေးခြင်း (Paper Certificate)

Root CA မှ သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူအဖြစ် ဆောင်ရွက်ရန်လိုင်စင်ရရှိသော CA သို့ ဒီဂျစ်တယ် သက်သေခံလက်မှတ်နှင့် အတူ သက်သေခံလက်မှတ်ရှိ အချက်အလက်များ ပါဝင်သောစာရွက် အထောက်အထားကိုပါ ထုတ်ပေးမည် ဖြစ်ပါသည်။

၄. ၄ သက်သေခံလက်မှတ်ကိုလက်ခံခြင်း (Certificate Acceptance)

၄. ၄. ၁ သက်သေခံလက်မှတ်ကိုရယူလက်ခံခြင်း (Conduct Constituting Certificate Acceptance)

CA သည် သက်သေခံလက်မှတ်အား Install ပြုလုပ်ပြီး သက်သေခံလက်မှတ်ကို အောင်မြင်စွာ Install ပြုလုပ်ပြီးကြောင်း၊ အသုံးပြုနိုင်ကြောင်းကို Root CA ထံသို့ (၁၅)ရက်အတွင်း ပြန်၍ အကြောင်းကြားစာ ပေးပို့ရမည် ဖြစ်ပါသည်။ Root CA မှ ထိုသို့အကြောင်းကြားစာ လက်ခံရရှိသည့်အခါ သက်သေခံလက်မှတ်ကို လက်ခံသည်ဟု သတ်မှတ်ပါသည်။ Root CA သို့ အကြောင်းကြားစာ မပြန်ရသေးခင် အချိန်အတွင်း သက်သေခံလက်မှတ်ကို Subscriber များသို့ လက်မှတ်ရေးထိုး ထုတ်ပေးခြင်းမပြုရပါ။ CA သည်သက်သေခံလက်မှတ်ကို ထုတ်ယူနိုင်ကြောင်း အကြောင်းကြားစာရရှိသည့်နေ့မှစ၍ ရက်ပေါင်း (၃၀) အတွင်း Root CA ထံလာရောက် ထုတ်ယူရမည်။ သတ်မှတ်ရက် ကျော်လွန်သွားပါက လိုအပ်သလိုဆောင်ရွက်နိုင်ရန် Root CA မှ ကြီးကြပ်မှု အဖွဲ့သို့ တင်ပြ၍ ညွှန်ကြားချက်တောင်းခံ ဆောင်ရွက်ပါသည်။

၄. ၄. ၂ သက်သေခံလက်မှတ်များအားထုတ်ပြန်ပေးခြင်း (Publication of Certificate by the Root CA)

Root CAသည် ထုတ်ပေးလိုက်သော သက်သေခံလက်မှတ်များအား အများပြည်သူကြည့်ရှုနိုင်ရန် အမျိုးသားသက်သေခံ လက်မှတ်မှတ်တမ်းတိုက် (National Repository) တွင် ထုတ်ပြန်ကြေငြာပေးထားမည် ဖြစ်ပါသည်။

၄. ၅ Key များနှင့် သက်သေခံလက်မှတ်အသုံးပြုမှု (Key Pair and Certificate Usage)

၄. ၅. ၁ CA ၏ Private Key နှင့် သက်သေခံလက်မှတ်အသုံးပြုမှု (CA Private Key and Certificate Usage)

CA သည် Root CA နှင့် လက်မှတ်ရေးထိုးထားသော ဌားရမ်းသုံးစွဲသူ၏သဘောတူညီချက် (Service User Agreement)၊ ဤ CP၊ CPS တို့တွင်ပါဝင်သည့် သတ်မှတ်ချက်များအတိုင်း သက်သေခံလက်မှတ်ကို သုံးစွဲရမည်။ သက်သေခံလက်မှတ်တွင်ပါဝင်သော Key Usage Field Extension နှင့် သက်သေခံလက်မှတ်အား အသုံးပြုခြင်းတို့သည် ကိုက်ညီမှုရှိရမည်။ CA များသည် မိမိတို့၏ Private Key များကိုအခွင့်မရှိသောသူမှ အသုံးမပြုနိုင်ရန် ဆောင်ရွက်ထားရမည်။ သက်တမ်းကုန်ဆုံးပြီးနောက်ပိုင်းနှင့် ပယ်ဖျက်ပြီးနောက်ပိုင်းတွင် ထိုသက်သေခံလက်မှတ်ကို ဌားရမ်းသုံးစွဲသူများသို့ သက်သေခံလက်မှတ်ထုတ်ပေးခြင်း၊ သက်တမ်းတိုးခြင်း၊ ပယ်ဖျက်ခြင်းဆိုင်ရာလုပ်ငန်းများအတွက် ဆက်လက် အသုံးမပြုရပါ။

၄. ၅. ၂ Relying Party မှ Public Key နှင့်သက်သေခံလက်မှတ်အသုံးပြုမှုများ (Relying Party Public Key and Certificate Usage)

Relying Party များသည် သက်သေခံ လက်မှတ်ကို ယုံကြည်အသုံးပြုခြင်းပြုလုပ်ရာတွင် Relying Party Agreement တွင်ရေးသားထားသော အချက်အလက်များကို သဘောတူရမည်။

သက်သေခံလက်မှတ် တစ်ခုပေါ်တွင် ယုံကြည်သုံးစွဲမှုသည် အခြေအနေအမျိုးမျိုးပေါ်မူတည်၍ အကြောင်းအကျိုး သင့်လျော်မှု ရှိ/မရှိ ကို Relying Party များကိုယ်တိုင် စဉ်းစား၊ ဆုံးဖြတ်၍ လက်ခံရမည်။ အကယ်၍ အခြေအနေတစ်ခုသည် နောက်ထပ်အာမခံချက်များ ရယူသင့်သည် ဟုယူဆပါက Relying Party သည် ထိုသို့ယုံကြည်သုံးစွဲခြင်းပြုလုပ်ရန်အတွက် လိုအပ်သောအာမခံချက်များကို ထပ်မံရယူရမည် ဖြစ်ပါသည်။

ထိုကဲ့သို့ ယုံကြည်သုံးစွဲမှုများ မပြုလုပ်မီ Relying Party သည် အောက်ပါအချက်တို့ကို လွတ်လပ်စွာ သုံးသပ်ခြင်း (assess) ပြုလုပ်ရမည်။

- ပေးထားသော ရည်ရွယ်ချက်အတွက် သက်သေခံလက်မှတ်အားအသုံးပြုခြင်းမှာ သင့်လျော်မှု ရှိမရှိ ၊
- ဤ CP မှ တားမြစ်၊ ကန့်သတ်ထားခြင်းမရှိသော သင့်တော်သည့် ရည်ရွယ်ချက်တစ်ခုအတွက် အမှန်တကယ် အသုံးပြုခြင်းဟုတ်၊ မဟုတ်၊
- သက်သေခံလက်မှတ်တွင်ပါဝင်သော KeyUsage Field Extension နှင့်ကိုက်ညီစွာ သက်သေခံလက်မှတ်ကိုအသုံးပြုခြင်း ဟုတ်၊ မဟုတ် များကို ဆုံးဖြတ်ရမည်။
- သက်သေခံလက်မှတ်နှင့် Certificate Chain တွင်ပါဝင်သောသက်သေခံလက်မှတ်အားလုံး၏ Status ကို စစ်ဆေးခြင်း။

Root CAသည် သက်သေခံလက်မှတ် အသုံးပြုခြင်း၏ သင့်လျော်မှု ကို စစ်ဆေးရန် တာဝန်မရှိပါ။ သက်သေခံလက်မှတ်သုံးစွဲမှုသည် သင့်လျော်သည်ဟု ယူဆလျှင် Relying Party များသည် သင့်လျော်သည့် Software နှင့်/(သို့) Hardware ကိုအသုံးပြု၍ ဒစ်ဂျစ်တယ်လက်မှတ်မှန်ကန်ကြောင်းစစ်ဆေးမှု (Digital Signature Verification) ကို ပြုလုပ်ခြင်းသော် လည်းကောင်း၊ အခြားသော Cryptographic Operation ကို အသုံးပြု၍သော်လည်းကောင်း သက်သေခံ လက်မှတ်၏မှန်ကန်မှုကို စစ်ဆေးရမည်။ သက်သေခံ လက်မှတ်မှန်ကန်ကြောင်းစစ်ဆေးဆောင်ရွက်မှုများနှင့် သက်သေခံလက်မှတ် အပေါ် တွင် ယုံကြည်သုံးစွဲမှုတို့သည် ဆက်စပ်ပါသည်။ ထိုကဲ့သို့ပြုလုပ် စစ်ဆေးဆောင်ရွက် ခြင်းတွင် Certificate Chain တွင်ပါဝင်သော သက်သေခံ လက်မှတ် အားလုံး၏ Digital Signature များ မှန်ကန်ကြောင်း စစ်ဆေးခြင်းတို့လည်း ပါဝင်ပါသည်။

၄. ၆ သက်သေခံလက်မှတ် သက်တမ်းတိုးခြင်း (Certificate Renewal)

Certificate Renewal ဆိုသည်မှာ သက်သေခံလက်မှတ်ကို သက်တမ်းတိုးခြင်း ပြုလုပ်ရာတွင် သက်သေခံလက်မှတ်တွင်ပါဝင်သော Public Key (သို့မဟုတ်) အခြား Information များကို ပြောင်းလဲခြင်းမရှိဘဲ ဌားရမ်းသုံးစွဲသူ CA အား သက်သေခံလက်မှတ် အသစ်တစ်ခုထုတ်ပေးခြင်းဖြစ်ပါသည်။ Certificate Renewal သည် လက်ရှိ Key Pair အားအသုံးပြုပြီး သက်သေခံလက်မှတ် သက်တမ်းတိုးလျှောက်တားခြင်းမျိုးဖြစ်ပါသည်။

သက်တမ်းတိုးခြင်းကို သက်သေခံလက်မှတ် သက်တမ်းမကုန်ဆုံးမီ (၃) လ ကြိုတင် လျှောက်ထားရမည်။ Key Pair သက်တမ်း(၃) နှစ်ပြည့်ပြီးပါက Key Pair အသစ်တစ်စုံ သုံး၍ သက်သေခံလက်မှတ်အသစ်ပြုလုပ်ရန် Root CA ထံ လျှောက်ထားရမည်။

၄. ၆. ၁ သက်သေခံလက်မှတ် သက်တမ်းတိုးခြင်းအခြေအနေ (Circumstances for Certificate Renewal and Re-Key))

CA ၏ လက်ရှိ သက်သေခံလက်မှတ်သက်တမ်းမကုန်ဆုံးမီ ထိုသက်သေခံလက်မှတ်အသုံးပြုခြင်းကို ဆက်လက်ဆောင်ရွက်နိုင်ရန်အတွက်သက်သေခံလက်မှတ်အသစ်တစ်ခုကိုသက်တမ်းတိုးပြုလုပ်ရန် လိုအပ်ပါသည်။

ဌားရမ်းသုံးစွဲသူ၏ လက်ရှိသက်သေခံလက်မှတ်၏သက်တမ်းမကုန်ဆုံးမီ သက်သေခံလက်မှတ်ကို ဆက်လက် အသုံးပြုနိုင်ရန်အတွက် ဌားရမ်းသုံးစွဲသူမှ သက်သေခံလက်မှတ်သက်တမ်းတိုးခြင်း (Re-Key or Renewl) လျှောက်ထားခြင်း ပြုလုပ်ရန် လိုအပ်ပါသည်။

၄. ၆. ၂ သက်သေခံလက်မှတ် သက်တမ်းတိုးလျှောက်ထားခွင့်ရှိသူ (Who Can Request Renewal?)

သက်သေခံလက်မှတ်လျှောက်ထားသူကိုယ်တိုင်မှသာလျှင် သက်သေခံလက်မှတ် သက်တမ်းတိုး ပြုလုပ်ရန် တောင်းဆိုနိုင်ပါသည်။

၄. ၆. ၃ သက်သေခံလက်မှတ် သက်တမ်းတိုးခြင်းဆောင်ရွက်မှု (Processing Certificate Renewal Request)

သက်တမ်းတိုး ပြုလုပ်ရာတွင် **Root CA** သည် မူလလျှောက်ထားခဲ့သူ အမှန်တကယ်ဖြစ်ကြောင်း သေချာစေရန် ပြန်၍စစ်ဆေးပါသည်။ ကြီးကြပ်မှုအဖွဲ့၏ ခွင့်ပြုချက်ဖြင့်သာ **Root CA** မှ သက်တမ်းတိုး လျှောက်ထားခြင်းကို ဆောင်ရွက်ပါသည်။ သက်တမ်းတိုးလျှောက်လွှာ ဖြည့်စွက်ပြီးသောအခါယခင် လျှောက်ထားစဉ်က ဖြည့်သွင်းခဲ့သော အချက်အလက်များအတိုင်း ပြောင်းလဲမှုမရှိခဲ့လျှင် သက်တမ်းတိုး သက်သေခံလက်မှတ်ကို ထုတ်ပေးပါသည်။

သက်တမ်းတိုး သက်သေခံလက်မှတ် လျှောက်ထားလာသည့်အခါတိုင်းတွင် မူလ သက်သေခံလက်မှတ် လျှောက်ထားစဉ်က ကြီးကြပ်မှုအဖွဲ့နှင့် ဤ CP တွင်သတ်မှတ်ထားသော စစ်ဆေးရမည့် အချက်များနှင့်အညီ **CA** ၏ Identity ကိုပြန်လည် စစ်ဆေး အတည်ပြုမည် ဖြစ်ပါသည်။

၄. ၆. ၄ သက်တမ်းတိုးပြီး သက်သေခံလက်မှတ်များကို ထုတ်ပြန်ကြေငြာပေးခြင်း (Publication of the Renewal Certification by the Root CA)

သက်တမ်းတိုး အသစ်ပြန်လည်ထုတ်ပေးလိုက်သော CA၏သက်သေခံလက်မှတ်ကို Root CA ၏ အများပြည်သူ ကြည့်ရှုနိုင်သောအမျိုးသားသက်သေခံလက်မှတ်မှတ်တမ်းတိုက် (National Repository) တွင်ထုတ်ပြန် ကြေငြာ ထားမည် ဖြစ်ပါသည်။

၄. ၇ Key Pair အသစ်ကိုအသုံးပြု ၍သက်သေခံလက်မှတ်သက်တမ်းတိုးခြင်း (Certificate Re-Key)

Certificate Re-Key သည် Public Key အသစ်တစ်ခုကို အသုံးပြု၍ သက်သေခံလက်မှတ်ထုတ်ပေးခြင်းဖြစ်ပါသည်။ CA ၏ လက်ရှိအသုံးပြုနေသော Private Key လုံခြုံ စိတ်ချရမှုကို သံသယရှိသောအခါ (သို့) လက်ရှိသုံးစွဲနေသော Key များ၏သက်တမ်း (၃)နှစ် ပြည့်သောအခါတို့တွင် Certificate Re-Key ပြုလုပ်ရမည်ဖြစ်ပါသည်။ ထိုကဲ့သို့ သက်တမ်းတိုးခြင်းကို သက်သေခံလက်မှတ် သက်တမ်း မကုန်ဆုံးမီ (၃) လ ကြိုတင်လျှောက်ထားရမည်။

၄. ၇. ၁ သက်သေခံလက်မှတ်အသစ် ပြန်လည်ပြုလုပ်ရန်တောင်းဆိုခွင့်ရှိသူများ (Who May Request Certificate of a New Public Key)

CA ၏သက်သေခံလက်မှတ်သက်တမ်းတိုးခြင်းအတွက် မူလသက်သေခံလက်မှတ် လျှောက်ထားရာတွင် လက်မှတ်ရေးထိုးခဲ့သူ ကိုယ်တိုင်မှသာသက်သေခံ လက်မှတ်အသစ် ပြန်လည်ပြုလုပ်ရန် တောင်းဆိုနိုင်ပါသည်။ ကြီးကြပ်မှုအဖွဲ့၏ ညွှန်ကြားချက်ဖြင့်သာ **Root CA** မှ **Re-Key** ပြုလုပ်ပေးပါသည်။

၄. ၇. ၂ Key အသစ်အသုံးပြု၍သက်သေခံလက်မှတ်သက်တမ်းတိုးရန် တောင်းဆိုခြင်းကို ဆောင်ရွက်ခြင်း (Processing Certificate Re-Keying Requests)

ကြီးကြပ်မှုအဖွဲ့သည် သက်သေခံလက်မှတ် **Re-Keying** လျှောက်ထားသူသည် မူလသက်သေခံလက်မှတ် လျှောက်ထားသူအမှန်တကယ်ဖြစ်ကြောင်းစစ်ဆေးခြင်း နှင့် Authentication ဖြစ်ရန် အတွက် သတ်မှတ်ထားသော လိုအပ်ချက်များနှင့်လျော်ညီစွာ ပြန်လည်စစ်ဆေးခြင်းတို့ကို လုပ်ထုံးလုပ်နည်းများအတိုင်း သေချာစွာ စစ်ဆေးပြီးနောက် **Root CA**ထံသို့ အကြောင်းကြားစာပေးပို့မည် ဖြစ်ပါသည်။ ထိုသို့အကြောင်းကြားစာ လက်ခံရရှိသည့်အခါ **Root CA** မှ သက်သေခံလက်မှတ်အသစ်တစ်ခု ထုတ်ပေးမည် ဖြစ်ပါသည်။

၄. ၇. ၃ Publication of the Re-Keyed Certificate by the Root CA

သက်တမ်းတိုး ပြုလုပ်ပြီးသော သက်သေခံလက်မှတ်များကို Root CA ၏ အများပြည်သူ ကြည့်ရှုနိုင်သော National Repository တွင် ထုတ်ပြန်ကြေငြာထားမည်ဖြစ်သည်။

၄. ၈ သက်သေခံလက်မှတ်ပြုပြင်ပြောင်းလဲခြင်း (Certificate Modification)

၄. ၈. ၁ သက်သေခံလက်မှတ်ပြုပြင်ပြောင်းလဲမှုအခြေအနေများ (Circumstances for Certificate Modification)

သက်သေခံလက်မှတ်ပြုပြင်ပြောင်းလဲခြင်း (Modification)သည် ဌားရမ်းသုံးစွဲသူ**CA**၏ Public Key မှလွဲ၍ လက်ရှိ သက်သေခံလက်မှတ်တစ်ခုတွင်ပါဝင်သော အချက်အလက်များပြောင်းလဲမှုကြောင့် သက်သေခံလက်မှတ်အသစ် တစ်ခုထုတ်ပေးရန် အတွက် လျှောက်ထားခြင်းကို ရည်ညွှန်းပါသည်။

သက်သေခံလက်မှတ်ပြုပြင်ပြောင်းလဲခြင်းပြုလုပ်ရန် **CA**မှ ကြိုးကြပ်မှုအဖွဲ့သို့ လာရောက် လျှောက်ထားရမည်။ **Root CA** သည် ကြိုးကြပ်မှုအဖွဲ့မှ သဘောတူ ခွင့်ပြုကြောင်း အကြောင်းကြားစာရရှိပါက သက်သေခံလက်မှတ်အသစ် ထုတ်ပေးမည်ဖြစ်ပါသည်။ သက်သေခံလက်မှတ်ပြုပြင် ပြောင်းလဲခြင်း (Modification)သည် အပိုဒ် (၄. ၁) တွင် ဖော်ပြထားသော သက်သေခံလက်မှတ်လျှောက် ထားခြင်းနှင့် တူညီသည် ဟု စဉ်းစားပါသည်။

၄. ၈. ၂ သက်သေခံလက်မှတ်ပြုပြင်ပြောင်းလဲရန်တောင်းဆိုခွင့်ရှိသူ (Who May Request Certificate Modification)

အပိုဒ် (၄. ၁. ၁) အတိုင်းဆောင်ရွက်ပါသည်။

၄. ၈. ၃ သက်သေခံလက်မှတ်ပြုပြင်ပြောင်းလဲပေးရန်တောင်းဆိုမှုများကို ဆောင်ရွက်ခြင်း (Processing Certificate Modification Requests)

ကြိုးကြပ်မှုအဖွဲ့မှ ညွှန်ကြားချက်ရရှိသောအခါ **Root CA** သည် သက်သေခံလက်မှတ်ပြုပြင်ပြောင်းလဲရန် လျှောက်ထားသူ၏ လိုအပ်သော အချက်အလက်များအား စစ်မှန်မှုစစ်ဆေးခြင်း (Identification နှင့် Authentication) ကို အပိုဒ်(၃. ၂) အတိုင်း ပြုလုပ်ပြီး သက်သေခံလက်မှတ်ကို ထုတ်ပေးပါသည်။

၄. ၈. ၄ သက်သေခံလက်မှတ် အသစ်ထုတ်ပြီးကြောင်း CA သို့အကြောင်းကြားခြင်း (Notification of New Certificate Issuance to CA)

Root CA သည် သက်သေခံလက်မှတ် အသစ်ထုတ်ပြီးပါက လျှောက်ထားသူ **CA** ထံသို့ အကြောင်းကြားစာ ပေးပို့ပါမည်။

၄. ၈. ၅ ပြုပြင်ပြောင်းလဲပြီးသော သက်သေခံလက်မှတ်ကိုလက်ခံခြင်း (Conduct Constituting Acceptance of Modified Certificate)

အပိုဒ်(၄. ၄. ၁) အတိုင်းဆောင်ရွက်ပါသည်။

၄. ၈. ၆ ပြုပြင်ပြောင်းလဲပြီးသော သက်သေခံလက်မှတ်ကိုထုတ်ပြန်ပေးခြင်း (**Publication of the Modified Certificate by the Root CA**)

အပိုဒ်(၄. ၄. ၂) အတိုင်းဆောင်ရွက်ပါသည်။

၄. ၉ သက်သေခံလက်မှတ်ပယ်ဖျက်ခြင်း နှင့်ဆိုင်းငံ့ခြင်း (**Certificate Revocation and Suspension)**

၄. ၉. ၁ သက်သေခံလက်မှတ်ပယ်ဖျက်ခြင်းနှင့်ဆိုင်းငံခြင်းအတွက် အခြေအနေများ (**Circumstances for Revocation and Suspension)**

သက်သေခံလက်မှတ်ကို ယာယီဆိုင်းငံ့ခြင်း (suspension) ပြုလုပ်ပြီးမှသာ ပယ်ဖျက်ပါမည်။ သက်သေခံလက်မှတ်ကို ပယ်ဖျက်ရန်အတွက် ယာယီဆိုင်းငံ့ခြင်း (suspension) ပြုလုပ်ထားသောကာလအတွင်း လိုအပ်သော စစ်ဆေးမှုများကို ကြီးကြပ်မှုအဖွဲ့ နှင့် Root CA တို့ မှပြုလုပ်ပါသည်။ Root CA သည် CA သက်သေခံ လက်မှတ်ကိုပယ်ဖျက်ရန် ကြီးကြပ်မှုအဖွဲ့၏ ညွှန်ကြားချက်ကို ရရှိမှသာ ဆောင်ရွက်ပါသည်။ ယာယီဆိုင်းငံ့ကာလအတွင်း CA သည် ငှားရမ်းသုံးစွဲသူများသို့ သက်သေခံလက်မှတ် ထုတ်ပေးခြင်း၊ သက်တမ်းတိုးခြင်း၊ ပယ်ဖျက်ခြင်းဆိုင်ရာ လုပ်ငန်းများမပြုလုပ်ရပါ။ ဆိုင်းငံ့ထားသော သက်သေခံ လက်မှတ်ကို ပယ်ဖျက်ခြင်း (Revoke) (သို့မဟုတ်) ပြန်လည်အသုံးပြုခွင့် ပေးခြင်းများနှင့် စပ်လျဉ်း၍ ကြီးကြပ်မှုအဖွဲ့မှ ညွှန်ကြားချက်များပေးပြီး Root CA မှ လိုအပ်သလို လိုက်နာဆောင်ရွက်ပါသည်။

ယာယီဆိုင်းငံ့ခြင်း (**Suspension)** ပြုလုပ်သည့်အခါ အောက်ပါတို့ကိုပြုလုပ်ရမည်။

(၁) ကြီးကြပ်မှုအဖွဲ့မှ Suspension ပြုလုပ်ရသည့် အကြောင်းပြချက်ကို Root CA/CA သို့ပေးခြင်း၊

(၂) သက်သေခံလက်မှတ်ကို Suspension ပြုလုပ်ကြောင်း **Web site** တွင်ကြေငြာခြင်းနှင့် **ARL** ထုတ်ပြန်ခြင်း၊

(၃) သက်သေခံလက်မှတ်ကို Suspension ပြုလုပ်ကြောင်း ပြည်တွင်းရှိ အခြား CA များသို့ အကြောင်းကြားစာ ပေးပို့ခြင်း၊

အောက်ပါအခြေအနေများဖြစ်ပေါ်ခဲ့လျှင် CA များ၏ သက်သေခံလက်မှတ်များကို ကြီးကြပ်မှုအဖွဲ့သည် ဆိုင်းငံ့နှင့် ပယ်ဖျက်မည်ဖြစ် ပါသည်။

(၁) Root CA (သို့) CA မှ ယင်းတို့၏ Private Key ခိုးယူခံရခဲ့လျှင်ဖြစ်စေ ၊ ဖောက်ခံရသည်ဟု ယုံကြည်လျှင် (သို့) သံသယရှိလျှင်၊

(၂) Root CA မှ ငှားရမ်းသုံးစွဲသူ CA သည်လိုက်နာရမည့်စည်းကမ်းများ (သို့) Service User Agreement ပါ အချက်များကို ချိုးဖောက်သည်ဟု ယုံကြည်ပြီး အကြောင်းပြချက်များ၊ သက်သေများရှိခဲ့လျှင်၊

(၃) CA နှင့် ချုပ်ဆိုထားသော သဘောတူညီချက်စာချုပ်များ ရပ်စဲ/ ပြီးဆုံးသွားလျှင်၊

(၄) CA အဖွဲ့အစည်းသည် ဖျက်သိမ်းလျှင် (သို့) မရှိတော့လျှင်၊

(၅) သက်သေခံလက်မှတ်လျှောက်ထားရာတွင် ဖြည့်သွင်းထားသည့်အချက်များ မှားယွင်းနေလျှင်၊

(၆) သက်သေခံလက်မှတ်ထုတ်ပေးခြင်းမပြုမီ ပြည့်စုံရမည့်အချက်များ ပြည့်စုံအောင် ဆောင်ရွက်ခြင်း မရှိခဲ့လျှင်၊

(၇) ငှားရမ်းသုံးစွဲသူ၊ အဖွဲ့အစည်း CA အမည်၊ သက်သေခံလက်မှတ်တွင် ပါဝင်သော Common Name (CN)ပြောင်းလဲခဲ့လျှင်၊

(၈) သက်သေခံလက်မှတ်ပါ အချက်အလက်များ မှန်ကန်မှုမရှိကြောင်းနှင့် ပြောင်းလဲသွားကြောင်း စစ်ဆေးဖော်ထုတ် တွေ့ရှိခဲ့လျှင်၊

(၉) သက်သေခံလက်မှတ်ကို ဆက်လက်သုံးစွဲပါက Root CA နှင့် ၎င်း၏လက်အောက်ရှိ CA များအား ပြဿနာ ဖြစ်နိုင်ခဲ့လျှင်၊

(၁၀) CA သည်သက်သေခံလက်မှတ်ကို တရားမဝင်ထုတ်ယူထားကြောင်းတွေ့ရှိရလျှင်၊

(၁၁) CA လုပ်ငန်းမှ ရပ်စဲခြင်းခံရလျှင်၊

သက်သေခံလက်မှတ်ဆက်လက် သုံးစွဲမှုကြောင့် ပြဿနာဖြစ်နိုင်ခြင်း ရှိ၊ မရှိ ဆုံးဖြတ်ရာတွင် အောက်ပါ အချက်များကို ထည့်သွင်း စဉ်းစားမည်။

(၁) တိုင်တန်းမှု (Complaint) အရေအတွက်နှင့် သဘောသဘာဝ၊

(၂) တိုင်တန်းမှု ပြုလုပ်သူသည် မည်သူမည်ဝါဖြစ်သည်ကို ထည့်သွင်းစဉ်းစားခြင်း၊

(၃) လက်ရှိပြဋ္ဌာန်းထားသော သက်ဆိုင်သည့်ဥပဒေများ၊ လုပ်ထုံးလုပ်နည်းများနှင့် ကိုက်ညီမှု ရှိမရှိ၊

(၄) ငှားရမ်းသုံးစွဲသူမှ ဘေးအန္တရယ်ဖြစ်အောင် အသုံးပြုမှုများကြောင့် ဖြစ်ပေါ်လာသော တုံ့ပြန်မှုများ၊

CA သည် Private Key ခိုးယူခံရလျှင်(သို့) ချိုးဖောက်ခံရ (Compromise) သည် ဟုယူဆပါက (သို့) သိရှိပါက Root CA နှင့် ကြီးကြပ်မှုအဖွဲ့ထံသို့ အမြန်ဆုံး ဆက်သွယ်အကြောင်းကြားရမည်။

၄. ၉. ၂ သက်သေခံလက်မှတ်ပယ်ဖျက်ရန်၊ ဆိုင်းငံ့ရန် တောင်းဆိုခွင့်ရှိသူ (Who can Request Revocation and Suspension)

Root CA လက်အောက်ရှိ CA များ၏ သက်သေခံလက်မှတ်များကို ယာယီဆိုင်းငံ့၊ ပယ်ဖျက်ရန် ကြီးကြပ်မှု အဖွဲ့၏ခွင့်ပြုချက်ဖြင့် Root CA မှ ပြုလုပ်ပါသည်။ ကြီးကြပ်မှု အဖွဲ့ (သို့) Root CA (သို့) CA မှသာဆိုင်းငံ့၊ပယ်ဖျက်ရန် တောင်းဆိုနိုင်သည်။

၄. ၉. ၃ သက်သေခံလက်မှတ်ပယ်ဖျက်ရန်၊ ဆိုင်းငံ့ရန် တောင်းဆိုမှုလုပ်နည်း (Procedure for Revocation and Suspension Request)

Root CA မှသော်လည်းကောင်း၊ CA မှသော်လည်းကောင်း ဆိုင်းငံ့ခြင်းနှင့် ပယ်ဖျက်ခြင်း ပြုလုပ်လိုပါက တရားဝင်စာဖြင့် Request Formတွင် ဖြည့်စွက်၍ ကြီးကြပ်မှုအဖွဲ့သို့တင်ပြ လျှောက်ထားရမည်။

၄. ၉. ၄ သက်သေခံလက်မှတ် ပယ်ဖျက်ရန် ဆိုင်းငံ့ချိန် (Revocation Request Grace Period)

သက်သေခံလက်မှတ်အားပယ်ဖျက်ရန် ဆိုင်းငံ့ချိန်မထားပါ။

၄. ၉. ၅ သက်သေခံလက်မှတ် ပယ်ဖျက်ရန်တောင်းဆိုခြင်းအတွက် Root CA မှ ဆောင်ရွက်ရန်ကြာမြင့်ချိန် (Time within which Root CA must process the Revocation Request)

Root CA သည် Revocation Request ကို ကြီးကြပ်မှုအဖွဲ့ထံမှ ဆောင်ရွက်ပေးရန် ညွှန်ကြားစာရလျှင် (၁)ရက် အတွင်း သတ်မှတ်ထားသော အဆင့်များအတိုင်း လုပ်ဆောင်သွားပါမည်။

၄. ၉. ၆ Relying Parties မှသက်သေခံလက်မှတ် ပယ်ဖျက်ထားမှုအခြေအနေကိုစစ်ဆေးရန် လိုအပ်ချက်များ (Revocation Checking Requirements for Relying Parties)

Relying Party များသည် မိမိအသုံးပြုမည့် သက်သေခံ လက်မှတ်များ၏ စိတ်ချရမှုအခြေအနေ (Status) ကို စစ်ဆေးရမည်။ သက်သေခံလက်မှတ် ၏စိတ်ချရမှုအခြေအနေ (Certificate Status) ကို စစ်ဆေးရာတွင်-

၁။ နောက်ဆုံးထုတ်ပြန်ခဲ့သော ARL (Most recent ARL) ကို အသုံးပြု၍ စစ်ဆေးခြင်း၊

၂။ Web-based Repository (သို့) LDAP (သို့) အကယ်၍ OCSP (ရှိပါက) ၎င်းကိုအသုံးပြုခြင်းတို့ဖြင့် စစ်ဆေးနိုင်ပါသည်။

Relying Parties များသည် Root CA ၏ National Repository ရှိ ARL များ၊ OCSP responder (ရှိပါက) များကိုအသုံးပြု၍ သက်သေခံလက်မှတ်၏ စိတ်ချရမှုအခြေအနေ(Status)ကို စစ်ဆေးနိုင်သည်။

၄. ၉. ၇ ARL ထုတ်ပြန်ပေးမှု အကြိမ်အရေအတွက် (ARL Issuance Frequency)

Root CA သည် CA Certificate များ ပြောင်းလဲမှု မရှိသည့်တိုင်အောင် (၆)လတစ်ကြိမ် **ARL** ကို ထုတ်ပြန်ပေးမည်။ ARL ထဲရှိ သက်သေခံလက်မှတ်တစ်ခု သက်တမ်းကုန်ဆုံးခြင်း (expire) ဖြစ်လျှင် ၎င်းသက်သေခံလက်မှတ်ကို ARL မှ ထုတ်ပယ် ပေးမည်ဖြစ်ပါသည်။

၄. ၉. ၈ သက်သေခံလက်မှတ်ကိုပယ်ဖျက်ခြင်း အများဆုံးကြာမြင့်ချိန် (Maximum Latency for ARLs)

Root CA မှ သက်သေခံလက်မှတ်ကို ပယ်ဖျက်စာရင်းထုတ်ပြီးလျှင်ပြီးချင်း National Repository တွင်ထုတ်ပြန်ပေးပါသည်။

၄.၉.၉ သက်သေခံလက်မှတ်ပယ်ဖျက်ထားခြင်းရှိ/ မရှိကို On-line စစ်ဆေးခြင်း (On-line Revocation/ Status Checking Availability)

ARL များ နှင့်သက်သေခံလက်မှတ်စိတ်ချရမှု အခြေအနေ (Certificate Status) များ စစ်ဆေးခြင်းကို National Repository နှင့် LDAP/ OSCP Responder (ရရှိနိုင်လျှင်)သုံး၍ စစ်ဆေးနိုင်ပါသည်။ Web Address မှာ http://www.rootca.org.mm ဖြစ်ပါသည်။

၄.၉.၁၀ ပယ်ဖျက်ထားသော သက်သေခံလက်မှတ် ဟုတ်၊ မဟုတ် On-line စစ်ဆေးခြင်း ပြုလုပ်ရန်လိုအပ်ချက်များ (On-line Revocation Checking Requirements)

သက်သေခံလက်မှတ်ကို ယုံကြည်စိတ်ချ၍လက်ခံအသုံးပြုသူများ(Relying Party) များသည် မိမိလက်ခံအသုံးပြုမည့် သက်သေခံလက်မှတ်၏ ယုံကြည်စိတ်ချရမှုအခြေအနေ (status) ကိုစစ်ဆေးရမည်။ Relying Party သည် သက်သေခံ လက်မှတ်၏ ယုံကြည်စိတ်ချရမှုအခြေအနေကို နောက်ဆုံးထုတ်ပြန်ခဲ့သည့် သက်ဆိုင်သည့် ARL/CRL ကိုအသုံးပြု၍ စစ်ဆေးခြင်း မပြုလုပ်ပါက National Repository ရှိ သက်သေခံလက်မှတ် အခြေအနေ(သို့) အသုံးပြုနိုင်သည့် OCSP responder (ရှိပါက) တို့ကို အသုံးပြု၍ စစ်ဆေးရမည်။

၄.၉.၁၁ Key ချိုးဖောက်ခံရခြင်းနှင့် သက်ဆိုင်သော အထူးဆောင်ရွက်ချက်များ (Special Requirements Regarding Key Compromise)

Root CA သည်မိမိမှ သက်သေခံလက်မှတ်ထုတ်ပေးထားသော CA (သို့) ၎င်း CA လက်အောက်ရှိ Sub CA များ ၏ private key ချိုးဖောက်ခံရ (compromise) သည်ဟု တွေ့ရှိလျှင် (သို့) ထိုသို့ဖြစ်သည်ဟု အကြောင်းပြချက် သက်သေခိုင်လုံမှု ရှိလျှင် ၎င်း၏ Potential Relying Party များအား အကြောင်းကြားခြင်းကို တတ်နိုင်သမျှပြုလုပ်ပေးပါမည်။

၄.၁၀ သက်သေခံလက်မှတ်စိတ်ချရမှုအခြေအနေ ဝန်ဆောင်မှုများ (Certificate Status Services)

၄.၁၀.၁ သက်သေခံလက်မှတ်၏ လုပ်ငန်းဆောင်ရွက်မှုအခြေအနေ (Operational Characteristics)

အများနှင့်ဆိုင်သောသက်သေခံလက်မှတ် (Public Certificate) များ၏အခြေအနေကို Root CA/CA ၏ CPS တွင်ဖော်ပြ ထားသော URL ရှိ Website ၊ LDAP Directory နှင့် OCSP Responder (ရှိပါက) တို့တွင်ဖော်ပြထားမည်။

၄. ၁၀. ၂ သက်သေခံလက်မှတ်နှင့်ဆိုင်သောဝန်ဆောင်မှု ရရှိနိုင်မှု (Service Availability)

သက်သေခံလက်မှတ်စိတ်ချရမှုအခြေအနေ ဝန်ဆောင်မှုများ (Certificate Status Service) ကို (၂၄)နာရီ (၇)ရက် ပတ်လုံး (Internet ဆက်သွယ်မှု ပြတ်တောက်နေချိန် သို့မဟုတ် စနစ်ပြုပြင်ထိန်းသိမ်းရေး (System maintenance) ပြုလုပ်နေ သဖြင့် ယာယီရပ်ဆိုင်းထားချိန်တို့မှလွဲ၍) ရရှိနိုင်ရန် ဆောင်ရွက်ထားပါသည်။

၄. ၁၁ သက်သေခံလက်မှတ်ငှားရမ်း သုံးစွဲခြင်းကို အဆုံးသတ်ခြင်း (End of Subscription)

CA သည် အောက်ပါနည်းလမ်းများဖြင့် ငှားရမ်း သုံးစွဲခြင်းကို အဆုံးသတ်နိုင်သည်။

၁။ မိမိ၏ သက်သေခံလက်မှတ်ကိုအသစ်ပြန်လည်ပြုလုပ်ခြင်း (renewal) သို့မဟုတ် သက်တမ်းတိုးခြင်း (Re-Key) ပြုလုပ်ခြင်းမပြုဘဲ သက်တမ်းကုန်ဆုံးခွင့်ပြုခြင်း၊

၂။ သက်တမ်းမကုန်ဆုံးမီ မိမိ၏ သက်သေခံလက်မှတ်ကို ပယ်ဖျက်ခြင်း။

၄. ၁၂ Private Key ကို Escrow လုပ်ခြင်းနှင့် ပြန်လည်ရယူခြင်း (Key Escrow and Recovery)

Root CA သည် ယင်း၏ Private Key နှင့် CA ၏ Private Key များကို Recovery အတွက် Escrow မပြုလုပ်ပါ။

၅. အထောက်အပံ့များ၊ စီမံခန့်ခွဲခြင်းနှင့် လုပ်ငန်းဆောင်ရွက်ခြင်းဆိုင်ရာ ထိန်းချုပ်မှုများ (Facility, Management and Operational Control)

၅. ၁ Root CA လုပ်ငန်း၏ ရုပ်ပိုင်းဆိုင်ရာထိန်းချုပ်၊ စီမံထားရှိမှုများ (Physical Controls)

၅. ၁. ၁ စခန်းတည်နေရာနှင့် ဆောက်လုပ်ခြင်း (Site Location and Construction)

Root CA သည် ၎င်း၏လုပ်ငန်းများကို လုပ်ကိုင်ဆောင်ရွက်ရာတွင် လုံခြုံမှုရှိစေရန်၊ မသက်ဆိုင်သူများမှ ကျူးကျော်ဝင်ရောက်ခြင်း၊ အသုံးပြုခြင်းမရှိစေရန်၊ လျှို့ဝှက်သတင်းအချက်အလက်များနှင့် စနစ်များကို မသက်ဆိုင်သူများမှ ကြည့်ရှုခြင်းမပြုလုပ်နိုင်ရန် ရုပ်ပိုင်းဆိုင်ရာကာကွယ်သည့်ပတ်ဝန်းကျင် (Physically Protected Environment)ကို ထားရှိအသုံးပြု၍ ဆောင်ရွက်ပါသည်။ Root CA သည် လုံခြုံမှုရှိစေရန်အတွက် အခန်းများတည်ဆောက်ခြင်းကို အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေးဥပဒေ နှင့် ၎င်းနှင့်ဆက်စပ်သည့် နည်းဥပဒေများ၊ အမိန့်ကြော်ငြာစာများ၊ လမ်းညွှန်ချက်များအတိုင်း ဆောင်ရွက်ထားပါသည်။

၅. ၁. ၂ လုပ်ငန်းဆောင်ရွက်ရာ နေရာသို့ဝင်ရောက်ခြင်း (Physical Access)

Root CA သည် ၄င်း၏စနစ်လုံခြုံရေးအတွက် အဆင့် (Tier) များ ခွဲခြားပြီး လုံခြုံရေး စစ်ဆေးထားပါသည်။ အတွင်းပိုင်းရှိလုံခြုံမှု အဆင့်ပိုမြင့်သည့်နေရာ (Higher Tier) များကို ဝင်ရောက်အသုံးပြုရန် အပြင်ပိုင်းရှိ လုံခြုံမှုအဆင့် ပိုနိမ့်သည့် နေရာ (Lower Tier) များကိုဖြတ်ကျော်ပြီးမှ ဝင်ရောက်ရပါသည်။

Tier တိုင်းကိုဝင်ရောက်ရန် ဝန်ထမ်းကဒ်များ စစ်ဆေးပြီးမှသာ ဝင်ရောက်နိုင်ပါသည်။ ထိုအခန်းသို့ ဝင်ရောက်ခြင်းကို Digital Video Recorder ဖြင့် မှတ်တမ်းတင်ထားပါသည်။ လုံခြုံသည့်ဧရိယာ (Secured Area) အဖြစ်သတ်မှတ်ထားသောနေရာများသို့ တိုက်ရိုက်တာဝန်ရှိသူမှလွဲ၍ အခြားသူများအားဝင်ရောက် ခွင့်မပြုပါ။

Cryptographic Material များ ထုတ်ပေးသည့်(Create) ပြုလုပ်သည့်၊ သိမ်းဆည်း(Store)ထားသည့် နေရာများသို့ဝင်ရောက်ခြင်း၊ စစ်မှန်ကြောင်းအထောက်အထားစိစစ်ခြင်း(Authentication)ကို Biometricsနည်း ပညာသုံး၍ ထိန်းချုပ်ထားပါသည်။ Server များ၊ စာရွက်စာတမ်းများကို သော့ခတ်ထားသောမီးခံသေတ္တာများ (Locked Safes) ၊ ဘီဒို (Cabinet) များ၊ သက်ဆိုင်ရာ Container များထားရှိ၍သိမ်းဆည်းထားသိုမည်ဖြစ်ပါသည်။

လုံခြုံမှုအဆင့် (Tier) တိုင်းတွင် ဝင်ထွက်ခြင်းများ၊ အသုံးပြုမှုကိစ္စများကို လုံခြုံရေးမှတ်တမ်း (Log-File) များ ဖွင့်လှစ်ထားရှိ၍ မှတ်တမ်းတင်ထားမည် ဖြစ်ပါသည်။ အထူးတာဝန်ဖြင့် ဝင်ရောက်ရန် လိုအပ်သည့်ပုဂ္ဂိုလ်များဝင်ထွက်ခြင်းကိစ္စကို ကြီးကြပ်မှုအဖွဲ့၏ အသိအမှတ်ဖြင့် Root CA ၏ တာဝန်ခံမှခွင့်ပြုပေးမည် ဖြစ်ပါသည်။

Sensitive Root CA Operation များဖြစ်သည့် Certification Life-Cycle Process များကို တင်းကျပ်သည့် လုံခြုံရေးအစီအမံများ ထားရှိဆောင်ရွက်ပါသည်။ (Certification Life-Cycle Process များမှာ သက်သေခံလက်မှတ်ထုတ်ပေးခြင်းများ(Issuance)၊ သိမ်းဆည်းခြင်း (Storage)၊ Key နှင့် သက်သေခံလက်မှတ်တို့ ဆိုင်ရာ သက်တမ်းတိုးခြင်း၊ ဆိုင်းငံ့ခြင်း၊ ပယ်ဖျက်ခြင်း (Revocation) စသည်တို့ ဖြစ်ပါသည်။)

၅. ၁. ၃ မီးအားပေးစနစ်နှင့် လေအေးစက်ထားရှိဆောင်ရွက်မှု (Power and Air Conditioning)

- Root CA ၏ စနစ်(system) ဆက်တိုက်အလုပ်လုပ်နိုင်ရန် (Continuous and Uninterrupted Access) အတွက် လျှပ်စစ်ဓါတ်အားပြတ်တောက်သွားခြင်းမရှိစေရန် မီးအားပေးစနစ်တွင် အရံမီးစက်များထားရှိဆောင်ရွက်ပါသည်။
- အခန်းအပူချိန်၊ လေဝင်လေထွက်၊ လေအေးပေးစနစ်၊ စိုထိုင်းမှု (Humidity) တို့ကို Control System တစ်ရပ်ဖြင့် ထိန်းညှိပေးထားပြီး ယင်း System တွင်လည်း Primary နှင့် Backup စနစ်များဖြင့် ခွဲခြားစီစဉ် ဆောင်ရွက်ထားရှိပါသည်။

၅. ၁. ၄ ရေကြောင့်ပျက်စီးဆုံးရှုံးမှု (Water Exposures)

ရေကြောင့်ပျက်စီးဆုံးရှုံးမှု မရှိစေရန် လိုအပ်သည့်စီစဉ်ဆောင်ရွက်မှုများ ပြုလုပ်ထားပါသည်။

၅. ၁. ၅ မီးဘေးအန္တရာယ်မှကာကွယ်ခြင်း (Fire Prevention and Protection)

မီးဘေးအန္တရာယ်မှကာကွယ်နိုင်ရန် လိုအပ်သည့် ကိရိယာများတပ်ဆင်ခြင်းနှင့် ကာကွယ်ငြိမ်းသတ်မည့် အစီအစဉ်များ ရေးဆွဲစီမံဆောင်ရွက်ထားပါသည်။

၅. ၁. ၆ Media များထိန်းသိမ်းထားရှိမှု (Media Storage)

Software များ၊ Data များ၊ Backup Information များ၊ စာရင်းစစ် Log File များ၊ မှတ်တမ်း File များကို အခွင့်ရှိသူများသာ ကြည့်ရှုနိုင်ရန် စနစ်တကျ တားဆီးကာကွယ်သည့်စနစ်များ စီစဉ်ဆောင်ရွက်ထားပါသည်။ ရေ၊ မီး၊ အခြားသော သဘာဝဘေးအန္တရာယ်များနှင့်၊ သံလိုက်ဓါတ်များကြောင့် စာရွက်စာတမ်းများ၊ CD များ၊ စနစ်များပျက်စီးဆုံးရှုံးမှု မရှိစေရန် စီစဉ်ဆောင်ရွက်ထားပါ သည်။

၅. ၁. ၇ မလိုသည့်စွန့်ပစ်ပစ္စည်းများဖျက်စီးစွန့်ပစ်မှု (Waste Disposal)

Root CA သည် အသုံးမလိုသည့်စွန့်ပစ်ပစ္စည်းများကို စနစ်တကျစွန့်ပစ်မည့်နည်းလမ်းများ စီစဉ်ဆောင်ရွက်ထားပါသည်။ အရေးကြီးသည့် သတင်းအချက်များပါရှိသည့် စာရွက်စာတမ်းများ၊ CD များ၊ ပစ္စည်းကိရိယာများကို စွန့်ပစ်ခြင်းမပြုမီ သေချာစွာဖျက်ဆီးပြီးမှသာ စွန့်ပစ်ရန် စီစဉ်ထားပါသည်။ အရေးကြီးသော သတင်းအချက်အလက် (Sensitive Information) များပါရှိသည့် Mediaများ၊ စာရွက်စာတမ်းများကို ဖတ်ရှု၍ မရနိုင်ရန် ဖျက်ပြီးမှသာ စွန့်ပစ်ပါသည်။

၅. ၁. ၈ လုံခြုံစိတ်ချရသည့် အခြားနေရာတွင် Backup ပြုလုပ်သိမ်းဆည်းခြင်း (Off-Site Backup)

Root CA သည် Audit Log Data များနှင့် အရေးကြီးသည့်သတင်းအချက်အလက် (Sensitive Information) များပါဝင်သည့် အရေးကြီးသည့်စနစ် Data များကို လုံခြုံသည့် အခြားတစ်နေရာတွင် Backup ပြုလုပ် သိမ်းဆည်းထားပါသည်။

၅. ၂ လုပ်ငန်းဆိုင်ရာ ထိန်းချုပ်မှုများ (Procedural Controls)

၅. ၂. ၁ ယုံကြည်စိတ်ချရသူများကဏ္ဍ (Trusted Roles)

Root CA သည်ယုံကြည်စိတ်ချရသည့်နေရာ (TrustedPosition) တွင်တာဝန် ထမ်းဆောင်မည့် ယုံကြည်စိတ်ချရသော ပုဂ္ဂိုလ်များ(Trusted Person) ဟုသတ်မှတ်ရာတွင် အောက်ဖော်ပြပါ လုပ်ငန်းများကို ပါဝင် လုပ်ဆောင်ပါတ်သက်နေသည့် ဝန်ထမ်းများအားလုံး၊ စာချုပ်နှင့်လုပ်ငန်းလုပ်ကိုင်သူ (Contractors) များနှင့်

အကြံပေးအရာရှိ၊ အတိုင်ပင်ခံပုဂ္ဂိုလ် (Consultant)များ၊ ဗဟိုအဖွဲ့နှင် ကြီးကြပ်မှုအဖွဲ့မှ အမိန့်စာဖြင့် တရားဝင်တာဝန် ပေးအပ်ခြင်းခံရသူများအားလုံးအကျုံးဝင်ပါသည်။

Trusted Person များတွင် Root CA life-cycle လုပ်ငန်းများကို ဆောင်ရွက်သူများ၊ စနစ်လုံခြုံရေးကို တာဝန်ယူဆောင်ရွက်သူများ၊ စနစ်Authentication ကို Control လုပ်ခွင့်ရှိသူများနှင့် အောက်ဖော်ပြပါ လုပ်ငန်းတို့ကို လုပ်ကိုင်ဆောင်ရွက် နေသူများ ပါဝင်ပါသည်။

- Certificate Application တွင်ဖြည့်သွင်းထားသည့် အချက်အလက်များကို စစ်ဆေးသူ၊
- Certificate Application များ၊ Revocation Request/Suspension များ၊ Renewal Request (သို့) Enrollment Information များကို လက်ခံခြင်း၊ ပယ်ချခြင်း (သို့) Certificate Application ကို အခြားဆောင်ရွက်မှု တစ်ခုခုကို ပြုလုပ်သူများ၊
- သက်သေခံလက်မှတ်များကို ထုတ်ပေးခြင်း၊ ပယ်ဖျက်ခြင်း ၊ ဆိုင်းငံ့ခြင်း ဆောင်ရွက်သူများ (Signing Rorm, National Repository/ LDAP / OCSP (ရှိပါက)များ၏ ကန့်သတ် ထားသော နေရာများသို့ ဝင်ရောက်ပြုပြင်ပြောင်းလဲခြင်း၊ ထုတ်လုပ်ခြင်း၊ သုံးစွဲခြင်း အခွင့်ရှိသူအားလုံး)၊
- ငှားရမ်းသုံးစွဲသူ CA များနှင့်ပတ်သက်သောအချက်အလက်များ၊ Request များကိုကိုင်တွယ်ဖြေရှင်းသူများ၊
- Customer Service ကိုဆောင်ရွက်နေသောဝန်ထမ်းများ၊
- Cryptographic Service ကိုဆောင်ရွက်သောဝန်ထမ်းများ၊
- System Administrator များ၊
- သက်ဆိုင်သည့်အင်ဂျင်နီယာများ၊
- Infrastrature ၏လုံခြုံစိတ်ချရမှုအတွက် စီမံဆောင်ရွက်သူ အထက်အဆင့်အရာရှိများ ပါဝင်ပါသည်။

ထိုယုံကြည်စိတ်ချရသောပုဂ္ဂိုလ် (Trusted Person) များသည် သတ်မှတ်ထားသော အရည်အချင်းများ (Screening Requirement)နှင့် ပြည့်စုံကိုက်ညီမှုရှိရပါမည်။

၅. ၂. ၂ လုပ်ငန်းတစ်ခုချင်းစီအတွက်လိုအပ်မည့်ဝန်ထမ်းအရေအတွက် (**Number of Persons Required Per Task)**

Root CA သည် တင်းကျပ်သောလုပ်ထုံးလုပ်နည်း(Control Procedure) များသတ်မှတ်ထားရှိပြီး ထိုအတိုင်း ဆောင်ရွက်မှုရှိစေရန် တာဝန် (duty) များသီးခြားစီ ခွဲဝေချထားခြင်း၊ အရေးကြီးသည့် လုပ်ငန်းများတွင် ဝန်ထမ်းများ တစ်ဦးထက်မက တာဝန်ယူဆောင်ရွက်မှသာပြီးမြောက်ရန် တာဝန်ပေးထားခြင်းများဖြင့် ထိန်းချုပ်မှု (control) ပြုလုပ်ထားပါသည်။

အလုပ်တာဝန်အလိုက် တာဝန်ယူခွဲခြားဆောင်ရွက်မှု၊ သေချာမှုရှိစေရန်အတွက် လုပ်ထုံးလုပ်နည်း (Policy) များ၊ control procedure များထားရှိပါသည်။ အရေးကြီးဆုံးအလုပ်များဖြစ်သည့် Root CA ၏ Cryptographic ဆိုင်ရာ Hardware များ၊ HSM များ၊ Signing unit များ၊ သက်ဆိုင်သည့် key material များကို လူတစ်ဦးထက်မက ထားရှိပြီး လုပ်ဆောင်မှုသာ ပြီးမြောက်စေမည် ဖြစ်ပါသည်။

Internal control procedure များအနေဖြင့် လုံခြုံမှုအတွက် အရေးကြီးသည့် အချက်အလက်များ၊ စက်ပစ္စည်းကိရိယာများကို ကိုင်တွယ်ဆောင်ရွက်ရာတွင် (Physical Access or Logical Access အပါအဝင်) အနည်းဆုံး လူ(၂)ယောက် ထားရှိပြီး ဆောင်ရွက်မှသာ လုပ်ငန်းကိုပြီးမြောက်အောင် ဆောင်ရွက်နိုင်မည့် အစီအစဉ်များ ထားရှိဆောင်ရွက်ထားပါသည်။

သက်သေခံလက်မှတ် လျှောက်လွှာတစ်စောင်ရောက်လာသည်မှစ၍ စစ်ဆေးခြင်း၊ သက်သေခံလက်မှတ် ထုတ်ပေးခြင်း၊ သက်တမ်းတိုးခြင်း ၊ ဆိုင်းငံ့ခြင်း၊ ပယ်ဖျက်ခြင်း၊ နောက်ဆုံးတွင် ဖျက်ဆီးပစ်ခြင်း စသည့် life-cycle တစ်ခုလုံးကို ယုံကြည်စိတ်ချရသည့် ဝန်ထမ်းများထားရှိပြီး ဆောင်ရွက်ပါသည်။ ပစ္စည်းများကို ကိုင်တွယ်အသုံးပြု၍ လုပ်ငန်းလုပ်ဆောင်ရာတွင် တစ်ဦးတည်းနှင့် လုပ်ငန်းအစမှ အဆုံးသို့ ဆောင်ရွက်နိုင်ခြင်း မရှိစေရန် control များကိုခွဲဝေထားပါသည်။ Physical Access နှင့် Logical Access ကိုအရေးကြီးသည့် နေရာများတွင် သီးခြားလူများသုံး၍ ခွဲခြားဆောင်ရွက်ထားပါသည်။

၅. ၂. ၃ ဝန်ထမ်းတစ်ဦးချင်းစီ၏ လုပ်ငန်းတာဝန်များနှင့် စစ်ဆေးမှုကဏ္ဍ (Identification and Authentication for each Role)

Root CA ၏ ယုံကြည်စိတ်ချရသော ဝန်ထမ်းအဖြစ် ခန့်ထားမည့် လုံခြုံရေးအဆင့်မြင့်အရာရှိများ (Top Level security related)အားလုံးကို လူတွေ့စစ်ဆေးခြင်း၊ မှတ်ပုံတင်နှင့် အခြားလိုအပ်သော အထောက်အထားများအားစစ်ဆေးခြင်းများကိုသေချာစွာပြုလုပ်ပြီးကြိုးကြပ်မှုအဖွဲ့၏သဘောတူညီချက်ဖြင့်သာ ဝန်ထမ်းအဖြစ် ခန့်ထားပါသည်။ လိုအပ်ပါက Background Check များပြုလုပ်ပြီးမှ ခန့်ထားခြင်းပြုလုပ်ပါသည်။ ဝန်ထမ်းအဖြစ် ခန့်ထားပြီးနောက် သက်ဆိုင်ရာအထက် လူကြီး၏ သဘောတူညီချက် ရရှိပြီးမှသာ စာရွက်စာတမ်းများ၊ ကွန်ပျူတာနှင့် ဆက်စပ်ပစ္စည်းများ၊ Software များကို ကိုင်တွယ်သုံးစွဲ (Access) ခွင့်ပေးခြင်း၊ အီလက်ထရောနစ် data များကို ကြည့်ရှုခွင့်၊ လုပ်ငန်း လုပ်ဆောင် ခွင့်ပေးခြင်းများကို ပြုလုပ်ပါသည်။

၅. ၂. ၄ လုပ်ငန်းတာဝန်များခွဲဝေမှု (Roles Requiring Separation of Duties)

လိုအပ်သလိုပြဋ္ဌာန်းပါသည်။

၅. ၃ ဝန်ထမ်းပိုင်းဆိုင်ရာထိန်းချုပ်မှုများ (Personnel Controls)

ယုံကြည်စိတ်ချရသောဝန်ထမ်းအဖြစ် လျှောက်ထားသူများသည် ၎င်းတို့၏ နောက်ကြောင်းရာဇဝင် (background)၊ပညာအရည်အချင်း၊မိမိတာဝန်ယူဆောင်ရွက်မည့်လုပ်ငန်းနှင့်ပတ်သက်သော လုပ်ငန်းအတွေ့အကြုံ

တို့ကိုပြည့်ပြည့်စုံစုံ တင်ပြလျှောက်ထားရမည်။ လိုအပ်ပါက ယခင်လုပ်ငန်းများမှ ရှင်းလင်းမှု(clearance) ကိုယူရမည် ဖြစ်ပါသည်။ Trusted Position တွင်ရှိနေသည့်ဝန်ထမ်းများအား နောက်ကြောင်းရာဇဝင်စစ်ဆေးခြင်း (background check) ကို အနည်းဆုံး (၅)နှစ် တစ်ကြိမ် ပြန်လည် ပြုလုပ်ပါသည်။

၅. ၃. ၁ ဝန်ထမ်းများအတွက်သင်တန်းပို့ချမှုများ (Training Requirements)

Root CA ၏ ဝန်ထမ်းအဖြစ်ခန့်ထားသူများကို သင်တန်းပေးပြီးမှ ခန့်ထားမည် ဖြစ်ပါသည်။ သင်တန်းပေးရာတွင် တစ်ဦးချင်းစီ၏ လုပ်ငန်းတာဝန်အလိုက် အောက်ပါတို့ကို သင်ကြားပါမည်။

- 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

၅. ၃. ၂ သင်တန်းပြန်လည်ပို့ချခြင်းအကြိမ်အရေအတွက်နှင့်လိုအပ်ချက်များ (Retraining Frequency and Requirements)

လိုအပ်သလို ပြဌာန်းပါသည်။

၅. ၃. ၃ လုပ်ငန်းတာဝန်ခွဲဝေချထားခြင်းနှင့် လှည့်လည်ပြောင်းလဲချထားခြင်း အစီအစဉ် (Job Rotation Frequency and Sequence)

လိုအပ်သလို ပြဌာန်းပါသည်။

၅. ၃. ၄ အခွင့်မရှိဘဲဆောင်ရွက်မှုများကိုပိတ်ပင်တားမြစ်ခြင်း (Sanctions for Unauthorized Actions)

Root CA ၏ ဝန်ထမ်းများမှ အခွင့်မရှိဘဲဆောင်ရွက်မှုများ (သို့) Root CA ၏ ပေါ်လစီနှင့် လုပ်ထုံးလုပ်နည်းများဖောက်ဖျက်မှုများကို ကြိုးကြပ်မှုအဖွဲ့သို့တင်ပြပြီးအရေးယူဆောင်ရွက်ပါသည်။ ကျူးလွန်သည့် အကြိမ်ရေ နှင့် ဖောက်ဖျက်မှုအတိုင်းအတာပေါ်တွင်မူတည်၍ ထိုက်သင့်သောပြစ်ဒဏ်ပေးခြင်း၊ အလုပ်မှ ထုတ်ပယ်ခြင်း နှင့် တရားဥပဒေအရ အရေးယူခြင်းတို့အထိ ဆောင်ရွက်ပါသည်။

၅. ၃. ၅ လုပ်ငန်းခွင်တာဝန်ထမ်းဆောင်ရန် လိုအပ်သော စာရွက်၊ စာတမ်းများ (Documentation Supplied to Personnel)

သက်ဆိုင်ရာဝန်ထမ်းများအား လုပ်ငန်းခွင်တာဝန်ထမ်းဆောင်ရန် လိုအပ်သောလမ်းညွှန်များ၊ စာရွက်၊ စာတမ်းများကို ပေးထားပါသည်။

၅. ၄ စာရင်းစစ် မှတ်တမ်းပြုလုပ်ခြင်းအစီအမံများ (Audit Logging Procedures)

၅. ၄. ၁ မှတ်တမ်းသိမ်းဆည်းထားရမည့်အဖြစ်အပျက်များ (Types of Events Recorded)

Root CA သည် manual log (or) automatic log များထားရှိပြီး အောက်ဖော်ပြပါ အဖြစ်အပျက်များ အတွက် စာရင်းစစ် မှတ်တမ်းထားရှိပါသည်။

- Root CA Key Life-cycle Management Events
    - Key ထုတ်ပေးခြင်း backup ပြုလုပ်ခြင်း၊ သိမ်းဆည်းခြင်း၊ ပြန်လည်ဖော်ထုတ်ခြင်း၊ မှတ်တမ်း သိမ်းဆည်းခြင်း၊ ဖျက်စီးခြင်း (Key Generation, backup, storage, recovery, archival and destruction)
    - Cryptographic device များ၏ Life-Cycle Management ဆိုင်ရာ အဖြစ်အပျက်များ၊
    - သက်သေခံလက်မှတ်လျှောက်ထားခြင်း၊ သက်တမ်းတိုးခြင်း၊ ပယ်ဖျက်ခြင်းနှင့် re-key ပြုလုပ် ခြင်းများ၊
    - လုပ်ငန်းစဉ်လိုအပ်ချက်ဆိုင်ရာတောင်းဆိုမှုများ(Requests)ကို လက်ခံဆောင်ရွက်ပေးရာတွင် အောင်မြင်မှုများ (သို့) မအောင်မြင်မှုများ၊ စနစ်စမ်းသပ် ဆောင်ရွက်ချက်ဆိုင်ရာ မှတ်တမ်းများ (Test Records)၊
    - သက်သေခံလက်မှတ်များ Generate ပြုလုပ်ခြင်းမှတ်တမ်းများ၊
    - ARL ထုတ်ပေးခြင်းများ၊
- လုပ်ငန်းစနစ်လုံခြုံရေးဆိုင်ရာဖြစ်စဉ်များ-
    - PKI စနစ်သုံးစွဲမှုများ (အောင်မြင်မှု/မအောင်မြင်မှုများ)၊
    - လျှို့ဝှက်ဖိုင်များ၊ မှတ်တမ်းများဖတ်ခြင်း (read access)၊ ရေးခြင်း (write access)၊ ဖျက်ဆီးခြင်းများ(Deletion)၊
    - လုံခြုံရေးဆိုင်ရာမှတ်တမ်းများနှင့် ထိုမှတ်တမ်းများ (Security Profile) တွင် ပြောင်းလဲ ပြုပြင်ထားမှုများ၊
    - စနစ်ယာယီချို့ယွင်းခြင်း (crash) များ၊ Hardware failures များနှင့် အခြားသောပုံမှန်မဟုတ်သည့် ကိစ္စရပ် (anomalies) များ၊
    - Firewall နှင့် Router activity များ၊
    - Root CA လုပ်ငန်းခွင်တွင် Tier အလိုက် ဧည့်ဝင်၊ ဧည့်ထွက်ရှိမှုများ၊
- Log ဖိုင်တွင် ရေးသားမှတ်တမ်းထားသည့်အချက်အလက်များ

- အမှတ်စဉ်(သို့) Automatic journal entry များအတွက် sequence number၊
- ဝင်၊ထွက်သည့်နေ့ရက်၊ အချိန် နှင့် အကြောင်းအရာ၊
- မှတ်တမ်းစာအုပ်တွင် ရေးသွင်းရပါက မှတ်တမ်းတင်သူ၏အမည်၊

- ဗဟိုအဖွဲ့နှင့် ကြီးကြပ်မှုအဖွဲ့တို့မှ မှတ်တမ်းအဖြစ်သိမ်းဆည်းရန်လိုအပ်သည်ဟုညွှန်ကြားထားသော အချက်အလက်များ။

၅. ၄. ၂ မှတ်တမ်းများကို စီမံဆောင်ရွက်ခြင်းကြိမ်နှုန်း (Frequency of Processing Log)

အရေးပါသည့် လုံခြုံရေးဆိုင်ရာအဖြစ်အပျက်များ၊ ကိစ္စရပ်များအတွက် တစ်ပတ်လျှင် အနည်းဆုံး တစ်ကြိမ်စစ်ဆေးမှုများ ပြုလုပ်ပါသည်။ ၎င်းအပြင် Root CA သည် ၎င်း၏ Audit log file များမှသံသယ ဖြစ်နိုင်သည့် သမားရိုးကျမဟုတ်သော၊ ပုံမှန်မဟုတ်သော အဖြစ်အပျက်များကို အမြဲတမ်း စစ်ဆေးပြီး သတိပေးချက် ထုတ်ပြန်မှုများကို စုံစမ်းစစ်ဆေးခြင်းများ ပြုလုပ်ပါသည်။ လုပ်ငန်းဆိုင်ရာဆောင်ရွက်မှု log file ကိုပြန်လည်စစ်ဆေး (review)သည့် ကိစ္စရပ်များကိုလည်း မှတ်တမ်းထားရှိပါသည်။ Root CA ၏ လုပ်ငန်းဆိုင်ရာ မှတ်တမ်းများကို ကြီးကြပ်မှု အဖွဲ့သို့ တစ်လလျှင် တစ်ကြိမ် တင်ပြပါသည်။

၅. ၄. ၃ Audit log file များထိန်းသိမ်းထားရှိခြင်း

Audit log file များကိုမှတ်တမ်းတင်ပြီး အနည်းဆုံး(၁၂)လ ကြာသည်အထိ Root CA ၏လုပ်ငန်းလုပ်ဆောင်သည့် နေရာတွင်ထိန်းသိမ်းထားရှိပြီးနောက်ပိုင်းတွင် လုံခြုံစိတ်ချရသည့်နေရာ၌ အပိုဒ်(၅. ၅) တွင် ဖော်ပြထားသည့်အတိုင်း မှတ်တမ်း ဟောင်းအဖြစ် သိမ်းဆည်းထားရှိပါသည်။

၅. ၄. ၄ Audit log file များကိုကာကွယ်ခြင်း (Prevention of Audit Log)

Audit log file များရှိ မှတ်တမ်းများကို မသမာသူများမှ ဝင်ကြည့်ခြင်း၊ ပြင်ဆင်ခြင်း၊ ဖျက်ပစ်ခြင်း (သို့) အခြားမသမာသည့် ကိစ္စများမပြုလုပ်နိုင်ရန်အီလက်ထရောနစ်နည်းဖြင့်ကာကွယ်တားဆီးသည့်စနစ်များ ပြုလုပ်ထားပါသည်။

၅. ၄. ၅ Audit မှတ်တမ်းများ backup ဆောင်ရွက်မည့်အစီအစဉ် (Audit Log Backup Procedures)

Audit Log များကိုနေ့စဉ်လုပ်ငန်း လုပ်ဆောင်သမျှ backup ပြုလုပ်ပြီး တစ်ပတ်တစ်ကြိမ်အပြည့်အဝ (full) backup ပြုလုပ်ပါသည်။

၅. ၄. ၆ Audit များစုစည်းမှု စနစ် (Audit Collection System (Internal vs. External))

လိုအပ်သလို ပြဋ္ဌာန်းပါသည်။

၅. ၄. ၇ ထိခိုက်ပျက်စီးမှုဖြစ်ပေါ်နိုင်ခြေများကို တိုင်းတာစစ်ဆေးခြင်း (Vulnerability Assessments)

ဖြစ်နိုင်ခြေရှိသော ထိခိုက်ပျက်စီးမှုများကို အောက်ပါနေရာများတွင် တိုင်းတာစစ်ဆေးမှုပြုလုပ်ရမည်။ စနစ်တစ်ခုလုံး၏ ဖြစ်နိုင်သောပျက်စီးဆုံးမှုများ တိုင်းတာစစ်ဆေးခြင်းကိုအနည်းဆုံးတစ်နှစ်လျှင်တစ်ကြိမ် ပြုလုပ်ပါသည်။

(က) Root CA စနစ်၏ Software/ Hardware ပိုင်းများ ၊

(ခ) Physical Facilities များ၊

(ဂ) Network စနစ် များ၊

(ဃ) Root CA စနစ်၊

၅. ၅ Record များမှတ်တမ်းဟောင်းထားရှိမှု (Records Archival)

၅. ၅. ၁ မှတ်တမ်းဟောင်းအဖြစ်ထားရှိရမည့် မှတ်တမ်းအမျိုးအစားများ (Types of Records Archived)

Root CA သည် အောက်ဖော်ပြပါကိစ္စများအတွက် မှတ်တမ်းထားရှိပါသည်။

- စုဆောင်းရရှိသည့် စာရင်းစစ်အချက်အလက် (Audit Data) အားလုံး၊
- သက်သေခံလက်မှတ်ထုတ်ပေးခြင်းနှင့် သက်ဆိုင်သည့် စာရွက်စာတမ်း (Support Document) များအားလုံး၊
- Certificate Life-Cycle ဆိုင်ရာအချက်အလက်အားလုံး၊
- ဗဟိုအဖွဲ့နှင့် ကြီးကြပ်မှုအဖွဲ့၏ ညွှန်ကြားချက်ဖြင့် မှတ်တမ်းထားရှိရမည့်အခြားအချက်များ၊

၅. ၅. ၂ မှတ်တမ်းဟောင်းအဖြစ်ထိန်းသိမ်းထားရှိမည့်ကာလ (Retention Period for Archive)

Root CA ၏ သက်သေခံလက်မှတ် ထုတ်ပေးခြင်းဆိုင်ရာ မှတ်တမ်းများကို အနည်းဆုံး (၇)နှစ် ကြာ မှတ်တမ်းဟောင်းအဖြစ် သိမ်းဆည်းထားရှိပါသည်။

၅. ၅. ၃ မှတ်တမ်းဟောင်းများကို ကာကွယ်ထားရှိမှု (Protection of Archive)

ထိုသိမ်းဆည်းထားသည့် မှတ်တမ်းဟောင်းများကို အခွင့်ရှိသည့်သူများကိုသာ ကြည့်ရှုခွင့်ပြု၍ မသက်ဆိုင်သူများမှ ကြည့်ရှုခြင်း၊ ပြင်ဆင်ခြင်း၊ ဖျက်ဆီးခြင်း၊ မှတ်တမ်းများတွင် ပြုပြင်ခြင်းများမပြုလုပ်နိုင်ရန် ကာကွယ်ထားရှိပါသည်။ သတ်မှတ်ထားသည့် မှတ်တမ်းများ၏ သက်တမ်းအတွင်း ပျက်စီးမှုမရှိစေရန် စနစ်တကျ ထိန်းသိမ်း ထားရှိပါသည်။

၅. ၅. ၄ မှတ်တမ်းဟောင်းများ Backup ထားရှိမည့်အစီအစဉ် (Archive Backup Procedure)

သတင်းအချက်အလက်များကို မှတ်တမ်းဟောင်းအဖြစ် ထားရှိရာတွင် အများစုကို အီလက်ထရောနစ် Recordပုံစံဖြင့်ထားရှိပြီး၊လိုအပ်ပါက စာရွက်စာတမ်းပုံစံဖြင့် မိတ္တူကူး၍ထိန်းသိမ်းထားရှိမည်ဖြစ်ပြီး ပျက်စီးမှုမရှိ စေရန်လည်း အတတ်နိုင်ဆုံး စနစ်တကျစီစဉ် သိမ်းဆည်းထားရှိပါသည်။

၅. ၅. ၅ မှတ်တမ်းများ၏ အချိန်မှတ်သားခြင်းဆိုင်ရာ လိုအပ်ချက်များ (Requirements for Time-Stamping of Records)

သက်သေခံလက်မှတ်များ၊ ARL များ၊ အခြားသောပယ်ဖျက်ခြင်းဆိုင်ရာ မှတ်တမ်း(Revocation Database)များတွင် အချိန်နှင့် နေ့ရက်ကို မှတ်သားထားပါသည်။ Root CA computer system ၏ Time Clock ကို စုံစမ်းစစ်ဆေးမှုများတွင် ကိုးကားအသုံးပြုနိုင်ရန်အတွက် ဒေသစံတော်ချိန်နှင့်ကိုက်ညီမှုရှိစေရန် ဆောင်ရွက်ထားရှိပါသည်။ ထိုကဲ့သို့အချိန်ဆိုင်ရာမှတ်သားမှုများသည် Cryptographicပေါ်တွင် အခြေခံရန်မလိုပါ။

၅. ၅. ၆ မှတ်တမ်းအချက်အလက်များစုစည်းမှု (Archive Collection System (Internal or External))

Root CA ၏ ယုံကြည်စိတ်ချရသောဝန်ထမ်းများ(**Trusted Person, Level- 3**)နှင့် အထက်သာ မှတ်တမ်းအချက်အလက်များကို လုပ်ကိုင်ဆောင်ရွက်ခွင့်ရှိပါသည်။

၅. ၅. ၇ မှတ်တမ်းများရရှိမှု နှင့် စစ်ဆေးမှု လုပ်ငန်းစဉ်များ (Procedures to Obtain and Verify Archive Information)

အခွင့်ရှိသူများနှင့် ယုံကြည်စိတ်ချရသူများသာ မှတ်တမ်းဟောင်း(Archive Data) များကို ဝင်ရောက်ကြည့်ရှုနိုင်မည့် လုံခြုံရေးစနစ် ထားရှိပါသည်။ မှတ်တမ်းများကို ပြုပြင်ပြောင်းလဲသွားခြင်း ရှိမရှိ (Integrity) ကို တစ်နှစ်လျှင်တစ်ကြိမ် ပြန်လည်စစ်ဆေးပါသည်။

၅. ၆ Root CA Key Pair များအသစ်ပြုလုပ်ခြင်း (Key Changeover)

Root CA၏Keyသက်တမ်း(Maximum life time)မှာ (၇)နှစ်ဖြစ်ပါသည်။ ထိုသတ်မှတ်သက်တမ်းကို ကျော်လွန်ပါက Root CA Key Pair များကို လုပ်ငန်းတွင် ဆက်လက်အသုံးမပြုပါ။ Root CA Key Pair သက်တမ်း မကုန်ဆုံးမီ အနည်းဆုံး (၃)လ ကြိုတင်၍သက်တမ်းတိုးခြင်း ပြုလုပ်ရမည်။ ထိုသို့သက်တမ်းတိုးရန် Root CA Key Pair အသစ်တစ်စုံ ထုတ်ရမည်။ Root CA Key Pair အဟောင်းမှ Root CA Key Pair အသစ်သို့ ကူးပြောင်းရာတွင် လွယ်ကူချောမွေ့စွာ ကူးပြောင်းနိုင်ရန် Key ပြောင်းလဲခြင်း လုပ်ထုံးလုပ်နည်းများ (Key Changeover Procedure) များကို ကြိုတင်သတ်မှတ်ထားပါသည်။

- Key ပြောင်းလဲခြင်း မပြုလုပ်မီ Root CA သည် CA များသို့ သက်သေခံလက်မှတ်ထုတ်ပေးခြင်းကို ရက်ပေါင်း (၉၀) ကြိုတင်၍ ရပ်နားပါသည်။
- Certificate Key Pair ရပ်စဲလိုက်သည့် နောက်ပိုင်း CA များ၏ Certificate Request များကို Root CA Key Pair အသစ်သုံး၍ Sign ထိုးမည်ဖြစ်ပါသည်။
- Original key Pair သက်တမ်းကုန်ဆုံးခြင်း မဖြစ်မီအထိ ARL များကို Original Key Pair သုံး၍ ထုတ်ပြန်ပါသည်။
- သက်သေခံလက်မှတ်အဟောင်း သက်တမ်းမကုန်ဆုံးမီ (၃)လကြိုတင်၍ သက်သေခံလက်မှတ်အသစ်ကို ထုတ်ပြီး Suppliment အဖြစ်အသုံးပြုပါသည်။

၅. ၇ Root CA အချက်အလက်များ တိုက်ခိုက်ခံရမှုနှင့် ဘေးအန္တရာယ်ကျရောက်မှုများမှ ပြန်လည်နေရာချထားခြင်း (Compromise and Disaster Recovery)

၅. ၇. ၁ မတော်တဆမှုနှင့်ချိုးဖောက်ခံရမှုများကို ကိုင်တွယ်ဖြေရှင်းမည့် လုပ်ထုံးလုပ်နည်းများ (Incident and Compromise Handling Procedures)

Root CA သည် မတော်တဆမှုနှင့်ချိုးဖောက်ခံရမှုများကို ကိုင်တွယ်ဖြေရှင်းမည့် အစီအမံများ ဆောင်ရွက်ထားရှိ ပါသည်။ ယင်းအစီအမံတွင် အနည်းဆုံး အောက်ဖော်ပြပါအချက်များ ပါဝင်ပါသည်။

(၁) Root CA key ချိုးဖောက်၊ ခိုးယူခံရခြင်း၊ ပျက်ဆီးခြင်း၊

(၂) CA key ချိုးဖောက်၊ ခိုးယူခံရခြင်း၊ ပျက်ဆီးခြင်း၊

(၃) Root CA စနစ်နှင့် ကွန်ယက်အတွင်းသို့ မသမာသူများဝင်ရောက်ခြင်း၊ အချက်အလက်များ ပြုပြင်ခံရခြင်း၊ ဖျက်ဆီးခံရခြင်း၊ ခိုးယူခံရခြင်း၊

(၄) သက်သေခံလက်မှတ်ကို တရားမဝင်ထုတ်ယူခံရခြင်း၊ ဆိုင်းငံ့ခံရခြင်း၊ ပယ်ဖျက်ခံရခြင်း၊

Root CA သည် ပြဿနာများ ဖြစ်ပွားလာပါက ကြီးကြပ်မှုအဖွဲ့၏ လမ်းညွှန်မှုခံယူ၍ ဆောင်ရွက်ပါသည်။ ပြဿနာဖြစ်ပွားသည့်အချိန်မှစပြီး ဖြေရှင်းပြီးသည့်အချိန်အထိ ဆောင်ရွက်ချက်များကို ကြီးကြပ်မှုအဖွဲ့ထံသို့ အဆင့်တိုင်းကို အစီရင်ခံတင်ပြမည်ဖြစ်ပြီး Root CA မှ ကြီးကြပ်မှုအဖွဲ့ထံတင်ပြသည့် နှစ်စဉ်အစီရင်ခံစာတွင်လည်း အသေးစိပ်ဖော်ပြပေးပါမည်။

၅. ၇. ၂ ကွန်ပျူတာနှင့် ဆက်စပ်ပစ္စည်းများ၊ ဆော့ဝဲလ်နှင့် အချက်အလက်များ ပျက်စီးဆုံးရှုံးမှုကို ဆောင်ရွက်ခြင်း (Computing Resources, Software and/ or Data are corrupted)

ကွန်ပျူတာနှင့်ဆက်စပ်ပစ္စည်း(Computing Resources)များ၊ Softwareများ၊ dataများ စသည့်တို့တွင် ပျက်စီးဆုံးရှုံးမှု (corruption) များ ဖြစ်ပွားပါကကြီးကြပ်မှုအဖွဲ့သို့ အစီရင်ခံစာတင်ပြပြီး Root CA

၏ လုံခြုံရေးနှင့် မတော်မဆမှုများကို ကိုင်တွယ်ဖြေရှင်းမည့် လုပ်ထုံးလုပ်နည်းများ(Incident Handling Procedure)အရ ဆောင်ရွက်သွားမည် ဖြစ်ပါသည်။ ထိုလုပ်ထုံးလုပ်နည်းများတွင် ကွန်ပျူတာနှင့် ဆက်စပ်ပစ္စည်း (Computing Resources)များ၊ Softwareများ၊ dataများစသည့်တို့ကိုသင့်လျော်သည့်နေရာသို့ရွှေ့ပြောင်းခြင်း၊ မတော်တဆမှုကို စုံစမ်းစစ်ဆေးခြင်း (incident investigation) နှင့် ပြန်လည်ဖြေရှင်းမည့် နည်းလမ်းများ ပါဝင်ပါသည်။

၅.၃.၃ Private key ချိုးဖောက်ခံရခြင်းအတွက် ဆောင်ရွက်မှုလုပ်ငန်းစဉ်များ (Entity Private Key Compromise Procedures)

Root CA ၏ Private Key (သို့) Infrastructure များ ချိုးဖောက်ခံရခြင်း(Compromise) (သို့) ထိုသို့ ဖြစ်ပျက်သည်ဟု အထောက်အထားခိုင်လုံပါက Root CA မှ အဖွဲ့ဖွဲ့ပြီး အခြေအနေကို လေ့လာဆန်းစစ်ခြင်း၊ Action Plan ရေးဆွဲခြင်း၊ Action Plan အတိုင်း အကောင်အထည်ဖော်ခြင်းများကိုဗဟိုအဖွဲ့နှင့်ကြီးကြပ်မှုအဖွဲ့၏ သဘောတူညီချက်ဖြင့်ဆောင်ရွက်သွားမည် ဖြစ်ပါသည်။ အကယ်၍ RootCA ၏ သက်သေခံ လက်မှတ်ကို ပယ်ဖျက်ရန်လိုအပ်ပါက-

- ထိုသို့ပယ်ဖျက်ကြောင်းကို National Repository တွင်ထည့်သွင်းကြေငြာပြီးသက်ဆိုင်သူများအား တတ်နိုင်သမျှ အကြောင်းကြားပေးမည် ဖြစ်ပါသည်။
- Root CA အတွက် Key Pair အသစ်တစ်စုံ generate ပြုလုပ်ပြီး သက်သေခံလက်မှတ် အသစ်တစ်ခု ထုတ်ပေးမည်ဖြစ်ပါသည်။

၅.၃.၄ ဘေးအန္တရာယ်ဖြစ်ပွားပြီးနောက် လုပ်ငန်းများ ဆက်လက်လည်ပတ်နိုင်မှု စွမ်းရည် (Business Continuity Capabilities after a Disaster)

လူ(သို့)ဘေးအန္တရာယ်များကြောင့် ပျက်စီးဆုံးရှုံးမှု၊ ထိခိုက်မှုများဖြစ်ပွားသည့်အခါ လုပ်ငန်းဆက်လက်ဆောင်ရွက်နိုင်စေရန် Root CA စနစ်နှင့် Root CA၏ Private Key ကိုလည်း Backupပြုလုပ်၍ ထားရှိပါသည်။

၆. နည်းပညာဆိုင်ရာ လုံခြုံရေး ထိန်းချုပ်မှုများ (Technical Security Controls)

၆.၁ Key Pair ပြုလုပ်ခြင်း နှင့် Installation ပြုလုပ်ခြင်း (Key-pair Generation and Installation)

Root CA / CA Key Pair Generate ပြုလုပ်ရန်အတွက်စနစ်တကျရွေးချယ်ထားပြီး လုပ်ငန်း ကျွမ်းကျင်မှုအရည်အချင်း(Skill)ရှိသော၊လေ့ကျင့်ပေးထားသောသူများကိုသာခန့်အပ်ဆောင်ရွက်ပါသည်။ ယုံကြည်စိတ်ချရသည့်စနစ်ထားရှိကာလည်း ဆောင်ရွက်ပါသည်။ Root CA/CA Key Pair အားလုံးကို ကြိုတင်

သတ်မှတ်ထားသည့် သတ်မှတ်ချက်များအတိုင်း Generate ပြုလုပ်ပါသည်။ Key Generate ပြုလုပ်သည့် လုပ်ငန်းစဉ်ကို Internet နှင့် ပြင်ပ Network ချိတ်ဆက်ထားခြင်းမရှိသော သီးသန့်သတ်မှတ်ထားသည့် ကွန်ပျူတာတွင်သာ ပြုလုပ်မည်ဖြစ်ပြီး ၊ Key Pair Generation နှင့်သက်ဆိုင်သည့်လုပ်ငန်း (Activities) အားလုံးကို နေ့ရက်၊ အချိန်နှင့်တကွ မှတ်တမ်းထားရှိပြီး ပါဝင်လုပ်ဆောင်သူအားလုံးမှ လက်မှတ်ရေးထိုးပါသည်။ ထိုသို့ဆောင်ရွက်မှု အဆင့်ဆင့်ကို သတ်မှတ်ထားသည့်ကာလအထိ မှတ်တမ်းအဖြစ်လိုအပ်သလို စစ်ဆေးခြင်း၊ ပြန်လည်ကြည့်ရှုခြင်းများ ပြုလုပ်နိုင်ရန် သိမ်းဆည်းထားပါသည်။

၆. ၁. ၁ CA သို့ Private Key ပေးပို့ခြင်း (Private Key Delivery to CA)

Root CA မှ Key pair ထုတ်ပေးပါက Private Key ကို သက်သေခံလက်မှတ်ဌာနရမ်းသုံးစွဲသူ(CA) ကိုယ်တိုင် Root CA ၏ ရုံးသို့ လာရောက်၍ ထုတ်ယူရန် လိုအပ်ပါသည်။ Root CA သည် Private Key ကိုလုံခြုံစိတ်ချရမှုရှိစေရန် PKCS#12 ပုံစံဖြင့်သာ ပေးပါသည်။

၆. ၁. ၂ Root CA ၏ Public Key ကို Relying Parties များမှအသုံးပြုနိုင်ရန် စီစဉ်ဆောင်ရွက်ထားခြင်း (Root CA Public Key Delivery to Relying Parties)

Root CA ၏သက်သေခံလက်မှတ်နှင့်Root CAမှထုတ်ပေးထားသော သက်သေခံလက်မှတ်အားလုံးကို Root CA ၏ web-siteတွင် Download ပြုလုပ်နိုင်ရန်တင်ထားပါသည်။ ဌာနရမ်းသုံးစွဲသူများ၏ သက်သေခံလက်မှတ်ရှိ Certificate Chain တွင် Root CA ၏ သက်သေခံလက်မှတ်အပါအဝင် full Certificate Chain အားလုံးပါဝင်မည်ဖြစ်ပါသည်။ S/MIME Protocol ကိုအသုံးပြုသော Relying Party များနှင့် သက်သေခံလက်မှတ်အသုံးပြုသူများသည် ၎င်းတို့ရှိ Root CA သက်သေခံလက်မှတ်၏ Validityကို သိရှိရန် Certificate hash value ကို Web site ရှိ Hash Value နှင့် တိုက်ဆိုင်စစ်ဆေးရမည်။ Root CA သက်သေခံလက်မှတ်ကို CA များ၏ Web siteတွင်လည်း တင်ထားမည်ဖြစ်ပါသည်။

၆. ၁. ၃ Key ၏အရွယ်အစား (Key-Sizes)

Key-Pair များ၏ Private Key များကို Cryptanalysis ပြုလုပ်ခြင်းနည်းဖြင့် သိရှိအောင် ပြုလုပ်နိုင်ခြင်းမှ ကာကွယ်နိုင်ရန်အတွက် လုံလောက်သော Key အရှည် (key length) ထားရှိပါသည်။ Root CA ၏ Key Lenght မှာ (၄၀၉၆) bit RSA ဖြစ်ပါသည်။ CA Key Pair ၏ Size သည် (၂၀၄၈) bit ရှိရပါမည်။ လက်မှတ်ရေးထိုးရန်အတွက် အသုံးပြုသော Hash Algorithm မှာ SHA1 ဖြစ်ပါသည်။

၆. ၁. ၄ Public Key Prameter ပြုလုပ်ခြင်းနှင့် အရည်အသွေးစစ်ဆေးခြင်း (Public Key Prameters Generation and Quality Checking)

CA များသည် လိုအပ်သော Key များကို မိမိကိုယ်တိုင် Generate ပြုလုပ်ပါက ကြီးကြပ်မှုအဖွဲ့မှ လက်ခံသော အလားတူစံသတ်မှတ်ချက်များအတိုင်း ပြုလုပ်ရမည်ဖြစ်ပါသည်။ Root CA မှ လက်ခံသော Generate ပြုလုပ်လိုက်သည့် Key Parameter များ၏ အရည်အသွေး (Quality) ကို FIPS 186-2 သို့မဟုတ် ကြီးကြပ်မှုအဖွဲ့မှလက်ခံသော သတ်မှတ်ချက်များအတိုင်း စစ်ဆေး (Verify) ပါမည်။

၆. ၁. ၅ Key အသုံးပြုရသည့်ရည်ရွယ်ချက် (Key Usage Purpose as per X.509 V3 keyUsage field)

Root CA ၏ **Key** ကို အောက်ပါရည်ရွယ်ချက်များဖြင့်အသုံးပြုပါသည်။

- **CA** များ၏သက်သေခံလက်မှတ်ကို လက်မှတ်ရေးထိုးထုတ်ပေးရန်နှင့်
- **ARL** များထုတ်ပေးရန်တို့ဖြစ်ပါသည်။

၆. ၂. Private Key ကာကွယ်ခြင်းနှင့် Cryptographic Module သုံးစွဲထိန်းချုပ်ခြင်းများ (Private Key Protection and Cryptographic Module Engineering Controls)

Root CA သည် Physical, Logical နှင့် Procedural Control များပေါင်းစပ်ကာ Root CA ၏ Private Key နှင့် CA များ၏ Private Key (ရှိပါက) များကို အမှန်တကယ်လုံခြုံစိတ်ချမှုရှိစေရန် စီမံဆောင်ရွက်ထားရှိပါသည်။ မိမိ၏ Private Key ပြင်ဆင်ခံရခြင်း၊ ပျောက်ဆုံးခြင်း၊ သူတပါးမှ အသုံးပြုခြင်းများ၊ မသက်ဆိုင်သူများမှ ကြည့်ရှုခြင်းများကို ကာကွယ်ရန် ကြိုတင် သတိပေးမှုများကို CA နှင့် သဘောတူညီချက် တွင် ရေးသား သတိပေးထားပါသည်။ Root CA မှ အသုံးပြုသော Hardware Cryptographic Module မှာ FIPS 140-1 (Level 3) နှင့် ကိုက်ညီမှု ရှိပါသည်။

၆. ၂. ၁ Cryptographic Module ၏အရည်အသွေးစံနှင့် ထိန်းချုပ်မှုများ (Cryptographic Module Standards and Controls)

သက်သေခံလက်မှတ်မူဝါဒများ(Certificate Policy) အရ Root CA သည် စနစ်လုံခြုံမှုအတွက် FIPS 140-1 (Level-3) Hardware Security Module ကို အသုံးပြုပါသည်။ CA များသည် ၎င်းတို့၏ (Certificate Policy) တွင် ဖော်ပြပါရှိချက်များအတိုင်း လိုက်နာ၍ သတ်မှတ်ချက်များနှင့်ကိုက်ညီသော Hardware Cryptographic Module ကို ရွေးချယ်သုံးစွဲရမည်။ Root CA သည် CA များမှရွေးချယ်ထားသော Hardware

Cryptographic Module ၏ စိတ်ချရမှုနှင့် အာမခံချက်ရှိ၊ မရှိကို လိုင်စင်ထုတ်ပေးခြင်းမပြုမီ ကနဦးစစ်ဆေးခြင်း (Initial Audit) ပြုလုပ်သည့်အချိန်၌ စစ်ဆေးပြီး ကြီးကြပ်မှုအဖွဲ့ထံ တင်ပြပေးရမည်ဖြစ်ပါသည်။

၆. ၂. ၂ Private Key ကို လူအများထိန်းချုပ်မှု (private key (m out of n) Multi-Person control)

လိုအပ်သလို ပြဋ္ဌာန်းပါသည်။

၆. ၂. ၃ Private Key Escrow ပြုလုပ်ခြင်း (Private Key Escrow)

Root CA နှင့် CA များ၏ Private Key များကို Escrow မပြုလုပ်ပါ။

၆. ၂. ၄ Private Key Backup

Root CA သည် ၎င်း၏ Private Key များကို သဘာဝဘေးအန္တရာယ်များ၊ အခြားသော အန္တရာယ်များ၊ ကျရောက်ပြီးသောအခါ လုပ်ငန်းဆက်လက်ဆောင်ရွက်နိုင်ရန် (Recovery ပြုလုပ်ရန်)အတွက်သာ ဤ CP ပါသတ်မှတ်ချက်များအတိုင်း Backup Copy ထားရှိပါသည်။ ထို Key များကို လျှို့ဝှက်ကုဒ်(Encrypt) ပြုလုပ်၍ Disaster Recovery Site တို့တွင်သိမ်းဆည်းထားရှိပါသည်။

၆. ၂. ၅ Private Key မှတ်တမ်းဟောင်းထားရှိမှု (Private Key Archival)

Root CA ၏ Private Key ကို Archive မပြုလုပ်ပါ။

၆. ၂. ၆ Private key ကို Cryptographic Module ထဲတွင် (သို့) Cryptographic Module မှ ပြောင်းရွှေ့ခြင်း (Private Key Transfer Into or From a Cryptographic Module)

Root CA သည် လက်မှတ်ရေးထိုးရန်အသုံးပြုမည့် မိမိ၏ Key Pair ကို Hardware Cryptographic Module အသုံးပြု၍ Generate ပြုလုပ်ပါသည်။ ၎င်းအပြင် ထို Key Pair ကို Recovery ပြုလုပ်ရန်အတွက် Encrypt ပြုလုပ်၍ သိမ်းဆည်းထားပါသည်။ ထို Key Pair ကိုအခြားသော Hardware Cryptographic Module သို့ပြောင်းရွှေ့ထားပါက Encrypt ပြုလုပ်ထားသည့် ပုံစံဖြင့်သာ တစ်ခုမှတစ်ခုသို့ ပြောင်းရွှေ့ခြင်း ပြုလုပ်ပါသည်။

၆. ၂. ၇ Private key ကို လျှို့ဝှက်ကုဒ်ပြောင်းí သိမ်းဆည်းခြင်း (Private Key Storage on Cryptographic Module)

Hardware Cyptographic Module(HSM) တွင် သိမ်းဆည်းထားသည့် Root CA ၏ Private Key များ ကို လျှို့ဝှက်ကုဒ်ပြောင်းထားသော (Encrypted) ပုံစံဖြင့်သာ သိမ်းဆည်းထားရှိပါသည်။

၆. ၂. ၈ Private key ကို Activation data သုံး၍ကာကွယ်ခြင်း (Method of Activating Private Key)

Root CA သည် ၎င်း၏ Private Key ဆုံးရှုံးခြင်း၊ ခိုးယူခံရခြင်း၊ ပြုပြင်ခံရခြင်း၊ အခွင့်မရှိသူများမှ သုံးစွဲခြင်း၊ ဖွင့်ကြည့်ခြင်းမရှိစေရန် (Activation) ပုံစံသုံး၍လည်း ကာကွယ်ထားပါသည်။

Private Key ကို အသုံးပြု၍ Sign ထိုးခြင်းပြုလုပ်နိုင်ရန် Activate ပြုလုပ်ရာတွင် Trusted Person အနည်းဆုံး (၂) ဦး ပါဝင်ပြုလုပ်မှသာ အောင်မြင်စေမည် ဖြစ်ပါသည်။

၆. ၂. ၉ Private key ကို Deactivation ပြုလုပ်ခြင်း (Method of Deactivating Private Key)

Root CA သည် Signing လုပ်ငန်းပြုလုပ်ပြီးသောအခါတိုင်း Activate လုပ်စဉ်တွင်ပါဝင်ခဲ့သော Trusted Person မှ Manual Shut Down ပြုလုပ်ခြင်း၊ Logout ပြုလုပ်ခြင်းဖြင့် Private key ကို Deactivate ပြုလုပ်ပါသည်။

၆. ၂. ၁၀ Private Key ကို ဖျက်ဆီးခြင်း (Method of Destroying Private Key)

Root CA သည် ၎င်း၏ Private Key ကို ဖျက်ဆီးရာတွင် HSM ကို ၎င်း၏စက်ရုံထုတ် မူလ အခြေအနေ(Factory Initial State)သို့ ပြောင်းလဲခြင်းနည်းဖြင့် ပြန်လည် တည်ဆောက်သုံးစွဲနိုင်ခြင်း မရှိစေရန် အကြွင်းအကျန်မရှိအောင် ဖျက်ဆီးပစ်ပါသည်။ ထိုသို့ ဖျက်ဆီးပစ်သည့်အခါတိုင်း မှတ်တမ်း Log ဖိုင်ထားရှိ မှတ်တမ်းတင်ထားပါသည်။ ထိုသို့ ဖျက်ဆီးခြင်းကို တစ်ဦးထက်မက ဆောင်ရွက်မှသာ ပြီးမြောက်စေရန် စီစဉ်ထားရှိပါသည်။

၆. ၃. Key Pair စီမံထိန်းသိမ်းခြင်းနှင့်သက်ဆိုင်သော အခြားနည်းလမ်းများ (Other Aspects of Key Pair Management)

၆. ၃. ၁ Public Key အားလုံးကို မှတ်တမ်းဟောင်းထားရှိမှု (Public Key Archival)

Root CA သည် ၎င်း၏ Public Key အားလုံးကိုမှတ်တမ်းဟောင်း(Archive)အဖြစ် သိမ်းဆည်းထားပါသည်။

၆. ၃. ၂ သက်သေခံလက်မှတ်နှင့် Key pair အသုံးပြုမှုကာလ(Certificate Operational Periods and Key Pair Usage Periods)

Root CA Certificate ၏ Operational Period သည် ပယ်ဖျက်ခြင်းမခံရပါက (၇) နှစ်ဖြစ်ပါသည်။ Key Pair များ၏ Operational Period သည် သက်သေခံလက်မှတ်များ၏ Validity Period အတိုင်း ဖြစ်ပါသည်။

ထို့အပြင် Root CA သည် ၎င်း၏ သက်သေခံလက်မှတ်သက်တမ်းမကုန်ဆုံးခင် (၃)လကြိုတင်၍ သက်သေခံလက်မှတ် အသစ်များထုတ်ပေးခြင်းကို ရပ်စဲပါသည်။

၆. ၄. Private Key Activation ပြုလုပ်ခြင်း (Activation Data)

၆. ၄. ၁ Private Key Activation ပြုလုပ်ခြင်း နှင့် Installation ပြုလုပ်ခြင်း (Activation Data Generation and Installation)

လိုအပ်သလိုပြဋ္ဌာန်းပါသည်။

၆. ၄. ၂ Activation ပြုလုပ်ရာတွင် သုံးသောအချက်အလက်များကို ကာကွယ်ခြင်း (Activation Data Protection)

လိုအပ်သလိုပြဋ္ဌာန်းပါသည်။

၆. ၄. ၃ Activation ပြုလုပ်ရာတွင် သုံးသောအချက်အလက်များနှင့် သက်ဆိုင်သော အခြားအကြောင်းအရာများ (Other Aspects of Activation Data)

လိုအပ်သလိုပြဋ္ဌာန်းပါသည်။

၆. ၄. ၃. ၁ Activation ပြုလုပ်ရာတွင် သုံးသောအချက်အလက်များပေးပို့ခြင်း (Acitvation Data Transmission)

လိုအပ်သလိုပြဋ္ဌာန်းပါသည်။

၆. ၄. ၃. ၂ Activation ပြုလုပ်ရာတွင် သုံးသောအချက်အလက်များများဖျက်ဆီးခြင်း(Activation Data Destruction)

လိုအပ်သလိုပြဋ္ဌာန်းပါသည်။

၆. ၅ ကွန်ပျူတာစနစ်လုံခြုံရေး ထိန်းချုပ်မှုများ (Computer Security Controls)

Root CA သည် ယင်းလုပ်ငန်းများ၏ ကွန်ပျူတာစနစ်အတွက် ယုံကြည်စိတ်ချရသည့်စနစ်ကို ကြီးကြပ်မှု အဖွဲ့မှ ဗဟိုအဖွဲ့၏ သဘောတူညီချက်ဖြင့် သတ်မှတ်ထားသည့် လုံခြုံရေးဆိုင်ရာ ညွှန်ကြားချက်များနှင့် အညီ ကိုက်ညီမှုရှိအောင် ဆောင်ရွက်ထားပါသည်။

၆.၅.၁ ကွန်ပျူတာလုံခြုံရေးအတွက် နည်းပညာဆိုင်ရာ သီးခြားလိုအပ်ချက်များ (Specific Computer Security Technical Requirements)

Root CA စနစ်သည် Root CA ၏ Software နှင့် Data File များကို မသက်ဆိုင်သူများမှ access မပြုလုပ်နိုင်ရန် ယုံကြည်စိတ်ချရသည့် စနစ်ထားရှိပါသည်။ ထို့အပြင် Key Generate ပြုလုပ်သော Computer ကို ကိုင်တွယ်သုံးစွဲခွင့်အား ကန့်သတ်ထားပြီး ခိုင်လုံသော အကြောင်းပြချက်ဖြင့်သာ သုံးစွဲခွင့်ပြုပါသည်။

Root CA ၏ Key Generate ပြုလုပ်သော Computer ကို Root CA ၏ ကျန်အစိတ်အပိုင်းများနှင့် သီးခြားခွဲထုတ်ထားပါသည်။ Password နှင့်စပ်လျဉ်း၍ အနည်းဆုံး Character အရေအတွက်ကိုလည်းကောင်း၊ Alphanumeric နှင့် Special Character များပေါင်းစပ်ပါဝင်ရန်လည်းကောင်း၊ Password များကို ပြောင်းလဲပေးရမည့်ကာလကိုလည်းကောင်း သတ်မှတ်ထားပါသည်။

Root CA ၏လုပ်ငန်းများနှင့်သက်ဆိုင်သည့် Database များ၊ Server များအား တိုက်ရိုက်ကိုင်တွယ်သုံးစွဲနိုင်ခွင့်ကို သတ်မှတ်ထားရှိသည့် ယုံကြည်စိတ်ချသူများကိုသာခွင့်ပေးထားပြီး ထိုသို့သုံးစွဲရန်မှာလည်း ခိုင်လုံသောအကြောင်း အချက် (Business Reason) ရှိရမည် ဖြစ်ပါသည်။ Primary နှင့် Remote Backup ကို Virtual Private Network (လုံခြုံမှုရှိသည့်စနစ်) ဖြင့်ထားရှိ ဆောင်ရွက်ပါသည်။

၆.၅.၂ ကွန်ပျူတာ လုံခြုံရေးအဆင့်အခြေအနေ (Computer Security Rating)

လိုအပ်သလိုပြဌာန်းပါသည်။

၆.၆ သက်သေခံလက်မှတ် ဖြစ်စဉ်ဆိုင်ရာ နည်းပညာထိန်းချုပ်မှု (Life Cycle Technical Controls)

လိုအပ်သလိုပြဌာန်းပါသည်။

၆.၇ Network လုံခြုံရေးဆိုင်ရာ ထိန်းချုပ်မှုများ (Network Security Controls)

Root CA သည် ၎င်း၏ လုပ်ငန်းများအားလုံးကို မသက်ဆိုင်သူများမှ ဝင်ရောက်၍ မသမာမှုများ မပြုလုပ်နိုင်ရန်လုံခြုံစိတ်ချရသည့် Network စနစ်ထားရှိဆောင်ရွက်ပါသည်။ မသက်ဆိုင်သူများအားကြည့်ရှုခွင့် မပြုသော Sensitive information များကို Root CA နှင့် CA၊ Root CA မှ Remote Site သို့ အချင်းချင်း

အပြန်အလှန်ပေးပို့ရာတွင် Encryption ပြုလုပ်၍သော်လည်းကောင်း၊ DigitalSignature များသုံးစွဲ၍သော်လည်းကောင်း ပေးပို့ ပါသည်။

Root CA သည်လုပ်ငန်းဆောင်ရွက်ခြင်းနှင့် ပြုပြင်ထိန်းသိမ်းခြင်း(Operation and Maintenance) ကို Off Line ပြုလုပ်ပြီး အခြားသော မည်သည့်ကွန်ပျူတာနှင့် ဆက်စပ်ပစ္စည်း (External Component) များနှင့်မှ ကွန်ယက်ချိတ်ဆက်ထားခြင်း မပြုလုပ်ပါ။ အမျိုးသားသက်သေခံလက်မှတ် မှတ်တမ်းတိုက် ဝန်ဆောင်မှုကို Online ထားရှိပြီး Internet အပါအဝင် အခြားသော ယုံကြည်စိတ်ချရမှုမရှိသည့် Network များနှင့် ချိတ်ဆက်ရာတွင် Firewall ကို အသုံးပြုထားပါသည်။

၆. ၈ အချိန်ဆိုင်ရာမှတ်တမ်းတင်ခြင်း (Time-Stamping)

သက်သေခံလက်မှတ်များ၊ ARL များနှင့် အခြားသော Revocation Database မှတ်တမ်းများတွင် လုပ်ဆောင်သည့် အချိန်နှင့်နေ့ရက်ကို မှတ်တမ်းထားရှိပါသည်။ ထိုကဲ့သို့ အချိန်ဆိုင်ရာမှတ်တမ်းများပြုလုပ်ခြင်းအတွက် Cryptographic နည်းစနစ် အသုံးပြုရန် မလိုအပ်ပါ။

၇. သက်သေခံလက်မှတ်၊ ARL နှင့် OCSP ဆိုင်ရာများ (Certificate, ARL and OCSP Profiles)

၇. ၁ သက်သေခံလက်မှတ်ဆိုင်ရာ Profile (Certificate Profile)

Root CA ၏ Certificate များသည်-

(a) ITU-T Recommendation X.509 Version 3

(b) RFC 3280 : Internet X.509 Public Key Infrastructure Certificate နှင့် CRL Profile, April 2002 (“RFC 3280”) တို့နှင့် ကိုက်ညီပါသည်။

၇. ၁. ၁ Version အမှတ်စဉ် (Version Number(s))

Root CA နှင့် CA များအတွက်ထုတ်ပေးသောCertificate Version မှာ X.509 version(3)ဖြစ်ပါသည်။

၇. ၁. ၂ သက်သေခံလက်မှတ် Extension (Certificate Extensions)

Root CA မှ ထုတ်ပေးသည့် သက်သေခံလက်မှတ်များ၏ **Certificate Extensions** များတွင် လိုအပ်သလို ဖြည့်ဆည်းထား ပါသည်။

၇. ၁. ၃ **Algorithm Object Identifiers**

Root CA သည် Certificate များကို အောက်ဖော်ပြပါ Algorithm များအသုံးပြု၍ Signing ပြုလုပ်ပါသည်။

- Sha-1 with RSA

၇. ၁. ၄ အမည်ပေးပုံစံ (**Name Forms**)

Root CA သည် Name Constraint Field ကို Subject Distinguised Name အတိုင်းဖြည့်သွင်းပါသည်။

၇. ၁. ၅ သက်သေခံလက်မှတ်အမည်ပေးခြင်းဆိုင်ရာ သတ်မှတ်ချက် (**Name Constraints**)

Root CA သည် Anonymous Name များ ခွင့်မပြုပါ။ အမည်များသည် အဓိပ္ပာယ်ရှိရမည့်အပြင် ဌားရမ်းသုံးစွဲသူ CA ၏ အမည်နှင့်လည်း ပတ်သက်မှု ရှိရမည်။ အမည်များသည် Unique Distinguished Name (DN) ဖြစ်ရပါမည်။

၇. ၁. ၆ သက်သေခံလက်မှတ်၏ပေါ်လစီဆိုင်ရာ ကိုယ်စားပြုချက် (**Certificate Policy Object Identifier**)

Certificate Policy Extension ကိုအသုံးပြုသည့်နေရာများတွင် ဤ CP အရထုတ်ပေးသည့် သက်သေခံလက်မှတ် အားလုံးတွင် ဤ Policy ကိုညွှန်းထားသည့် Object Identifier (OID) ထည့်သွင်းဖော်ပြပေးထားပါသည်။ ယခုပေါ်လစီ၏ OID တန်ဖိုးသည် အပိုဒ် (၁. ၂)တွင်ဖော်ပြထားချက်ပါအတိုင်းဖြစ်ပါသည်။

၇. ၁. ၇ ပေါ်လစီကန့်သတ်ချက်ဆိုင်ရာ အသုံးပြုမှု (**Usage of Policy Constraints Extension**)

ပြဋ္ဌာန်းထားခြင်းမရှိပါ။

၇. ၁. ၈ ပေါ်လစီအရည်အသွေးပုံစံနှင့် ဝေါဟာရအဓိပ္ပာယ်ဖွင့်ဆိုချက် (**Policy Qualifier Syntax and Semantics**)

ပြဋ္ဌာန်းထားခြင်းမရှိပါ။

၇. ၁. ၉ သက်သေခံလက်မှတ်၏ အရေးကြီးသော ပေါ်လစီဆိုင်ရာဝေါဟာရ အဓိပ္ပာယ်များကို ဆောင်ရွက်ခြင်း (**Processing Semantics for the Critical Certificate Policies Extension**)

ပြဋ္ဌာန်းထားခြင်းမရှိပါ။

၇. ၂ **ARL Profile**

ARL တွင်အောက်ဖော်ပြပါဇယားအတိုင်း Basic field များပါဝင်ပါသည်။

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

၇. ၂. ၀ Version Number (S)

Root CA သည် X.509 နှင့် Version 2 ARLs များကို Support ပြုလုပ်ပါသည်။ Version 2 ARLs များသည် RFC 3280 Requirements များနှင့်ကိုက်ညီမှုရှိပါသည်။

၇. ၂. ၂ ARL and ARL Entry Extensions

ပြဋ္ဌာန်းထားခြင်းမရှိပါ။

၈. ကိုက်ညီမှုရှိ၊ မရှိ စာရင်းစစ်ခြင်းနှင့် အခြားအကဲဖြတ်မှုများ (Compliance Audit and Other Assessment)

Root CA ၏လုပ်ငန်းဆောင်ရွက်မှုပုံစံအား ကြီးကြပ်မှုနှင့် ဗဟိုအဖွဲ့တို့ သဘောတူညီထားသည့် Security နှင့် Technical Guideline တွင်ဖော်ပြထားသည့် အချက်အလက်များအတိုင်း ကြီးကြပ်မှုအဖွဲ့မှ လိုအပ်သကဲ့သို့ စစ်ဆေးမှု ပြုလုပ်မည်ဖြစ်ပါသည်။ Root CA မှ လည်း ကြီးကြပ်အဖွဲ့၏ Compliance Audit ပြုလုပ်ရရှိမှုအရ ညွှန်ကြားသည့်အတိုင်း ဖြည့်ဆည်းဆောင်ရွက်သွားမည် ဖြစ်ပါသည်။

ဤအပိုင်းတွင် Root CA မှ IT System နှင့်ပါတ်သက်သော လုပ်ဆောင်မှုမှတ်တမ်းမှတ်ရာများကို သေချာစွာ စုစည်းသိမ်းဆည်းထားမည် ဖြစ်သည်။ မှတ်တမ်းမှတ်ရာများဟု ဆိုရာတွင် လုပ်ငန်းနှင့်ပါတ်သက်သော စာရွက်စာတမ်းများ၊ ဥပမာအားဖြင့်- လျှောက်လွှာ၊ အတည်ပြုသော စာရွက်စာတမ်းများ၊ အသုံးပြုမှု လက်စွဲစာရွက်စာတမ်းများ၊ လုပ်ပိုင်ခွင့်နှင့်ဆိုင်သော ပုံစံများ၊ မှတ်တမ်းစာအုပ်များ၊ မှတ်တမ်းဖိုင်များ၊ အခြားသင့်တော်သော မှတ်တမ်းပြုသင့် ထိန်းသိမ်းထားသင့်သည်များကိုဆိုလိုပါသည်။ ဤစာရွက်စာတမ်းများကို Audit Trial ရည်ရွယ်ချက်ဖြင့် သေချာစွာ ထိန်းသိမ်းထားမည် ဖြစ်သည်။ ထိုသို့ သိမ်းဆည်းထားခြင်း အားဖြင့်-

(က) လုံခြုံရေး(Security) ထိုးဖောက်လာသော ဖြစ်ပွားစေသည့်အကြောင်းရင်းများကို Log Documentation များရှိခြင်းဖြင့် သိရှိနိုင်မည်။

(ခ) ယခင်ကြုံတင်ချမှတ်ထားသောစည်းမျဉ်း (Rules and Regulations) များနှင့်လိုက်လျောညီထွေရှိမှု (သို့) သွေဖီမှုများကို သက်သေပြနိုင်မည်ဖြစ်သည်။

၈. ၁ အကဲဖြတ်မှုကြိမ်နှုန်းနှင့် အခြေအနေ (Frequency and Circumstance of Assessment)

ကြီးကြပ်မှုအဖွဲ့သည် Root CA အား (၁)နှစ်တွင် (၁)ကြိမ် စာရင်းစစ်ခြင်း ပြုလုပ်ပါသည်။

- Root CA သည် သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ CAများကို (၁)နှစ်တွင် (၁)ကြိမ် စာရင်းစစ်ခြင်း ပြုမည်ဖြစ်သည်။
- စာရင်းစစ်ခြင်းများကိုကြီးကြပ်မှုအဖွဲ့မှ လက်ခံသည့်အရည်အချင်းပြည့်ဝသည့် စာရင်းစစ် အဖွဲ့များ နှင့် စစ်ဆေးမည်။ စာရင်းစစ် အဖွဲ့တွင် လက်မှတ်ရ ပြည်သူ့စာရင်းကိုင် တစ်ဦးနှင့် Certified Information System Auditor တစ်ဦးပါရှိမည်ဖြစ်ပြီး ၄င်းတို့အနက်တစ်ဦးဦးသည် ဒီဂျစ်တယ် သက်သေခံလက်မှတ်များ နှင့် ဒီဂျစ်တယ်လက်မှတ်များ အကြောင်းလုံလောက်သော အသိပညာ၊ ဗဟုသုတရှိသူဖြစ်ရမည်။
- စာရင်းစစ်အဖွဲ့သည် သက်သေခံလက်မှတ် ထုတ်ပေးပိုင်ခွင့်ရှိသူ(CA)များနှင့် သီးခြားတည်ရှိမည်ဖြစ်ပြီး သက်သေခံ လက်မှတ် ထုတ်ပေးပိုင်ခွင့်ရှိသူ(CA)သို့ software များ၊ Hardware များ၊ ဝန်ဆောင်မှုများ၊ ကုန်ပစ္စည်းများ ရောင်းချနေသူများ မဖြစ်ရပါ။
- CA များသည် စာရင်းစစ်အဖွဲ့မှ လိုအပ်သော အချက်အလက်၊ စာရွက်စာတမ်းများနှင့် ဝန်ထမ်းများကို ပေးအပ်ရ မည်။

၈. ၂ အားနည်းချက်များပေါ်မူတည်၍ လုပ်ဆောင်ချက် (Action Taken as a Result of Deficiency)

စာရင်းစစ်ခြင်းရလဒ်အရ ချွင်းချက်(Exception) နှင့်အားနည်းချက် (Deficiencies) များရှိပါက ကြီးကြပ်မှုအဖွဲ့မှ ညွှန်ကြားသည့်အတိုင်း ဖြည့်ဆည်းဆောင်ရွက်ပေးပါမည်။

၉. အခြားသော စီးပွားရေးရာနှင့် ဥပဒေဆိုင်ရာ အကြောင်းအရာများ (Other Business and Legal Matters)

၉.၁ ပေးသွင်းရမည့် ငွေကြေးပမာဏ (Fees)

၉.၁.၁ သက်သေခံလက်မှတ် ထုတ်ပေးခြင်းနှင့် သက်တမ်းတိုးခြင်းအတွက် ပေးသွင်းရမည့်ငွေ (Certificate Issurance (or) Renewal Fees)

လိုအပ်သလို ပြဋ္ဌာန်းပါသည်။

၉.၁.၂ သက်သေခံလက်မှတ်ကို ကြည့်ရှုခြင်းအတွက် ကျသင့်ငွေ (Certificate Access Fees)

သက်သေခံလက်မှတ်များအား အမျိုးသားသက်သေခံလက်မှတ်မှတ်တမ်းတိုက် (National Repository) တွင်ထည့်သွင်းခြင်း (သို့) Relying Party များမှ အသုံးပြုနိုင်အောင် ပြုလုပ်ပေးခြင်းတို့အတွက် ကျသင့်ငွေ ကောက်ခံမည် မဟုတ်ပါ။

၉.၁.၃ သက်သေခံလက်မှတ်ပယ်ဖျက်စာရင်းနှင့် အခြေအနေကို ကြည့်ရှုခြင်းအတွက် ကျသင့်ငွေ (Revocation or Status Information Access Fees)

Root CA သည် Authority Revocation List (ARL) ပြုလုပ်ခြင်း၊ ထို ARL များကို Relying Party များမှ ကြည့်ရှုနိုင်ရန်ပြုလုပ်ပေးခြင်းတို့အတွက် ကျသင့်ငွေကောက်ခံမည် မဟုတ်ပါ။ သို့သော် အခြားသော value-added revocation information ဝန်ဆောင်မှုများအတွက် ကျသင့် ငွေကောက်ခံမည် ဖြစ်ပါသည်။ Root CA သည် အခြားသော Third party များမှ Revocation information များ၊ Certificate Status Information များ (သို့) National Repository တွင် time stamping ပြုလုပ်ခြင်းများကို Root CA နှင့် ကြီးကြပ်အဖွဲ့၏ စာဖြင့် ရေးသားခွင့်ပြုထားခြင်းမရှိပါက ခွင့်မပြုပါ။

၉.၁.၄ အခြားသောဝန်ဆောင်မှုများအတွက် ကျသင့်ငွေ (Fees for Other Services)

Root CA သည် ဤ CP နှင့် CPS ကိုဝင်ရောက်ကြည့်ရှုခြင်း(Access) လုပ်ခြင်းအတွက် ကျသင့်ငွေကောက်ခံခြင်းမရှိပါ။ Document များကိုကြည့်ရှုရုံမျှမဟုတ်ဘဲ ပြန်လည်ထုတ်ဝေခြင်း (Reproducation) ၊ ပြင်ဆင်ခြင်း (သို့) ၎င်းတို့ကိုအသုံးပြု၍ အခြားသော လုပ်ငန်းများ ဆက်လက်လုပ်ကိုင်ခြင်းကဲ့သို့သော အခြားသောရည်ရွယ်ချက်များဖြင့် အသုံးပြုလိုပါက Document များကို မူပိုင်ခွင့် (Copyright) ရှိသူ Root CA နှင့် လိုင်စင်သဘောတူညီချက် (Licence Agreement) ရယူရမည်။

၉. ၁. ၅ ပြန်အမ်းငွေပေးခြင်းဆိုင်ရာ မူဝါဒများ **(Refund policy)**

ပြဋ္ဌာန်းထားခြင်းမရှိပါ။

၉. ၂ ဘဏ္ဍာရေးဆိုင်ရာတာဝန်ယူမှု **(Financial Responsibility)**

CA များ၏ Public key များကို အသိအမှတ်ပြုပေးသော Root CA သည် မည်သည့် သက်သေခံလက်မှတ်ကိုမဆို အသုံးပြုခြင်းကြောင့်ဖြစ်ပေါ်လာသော ဆုံးရှုံးမှုအားလုံးအတွက် လျော်ကြေးငွေ (သို့) ပြန်အမ်းငွေပေးမည် မဟုတ်ပါ။ (Disclaim all liability.)

၉. ၂. ၁ အာမခံထားရှိမှု **(Insurance Coverage)**

ပြဋ္ဌာန်းထားခြင်းမရှိသေးပါ။

၉. ၂. ၂ အခြားသောပိုင်ဆိုင်မှု **(Assets)** များ **(Other Assets)**

ပြဋ္ဌာန်းထားခြင်းမရှိသေးပါ။

၉. ၂. ၃ အခြားသော အာမခံတွင်ပါဝင်မှုများ **(Extended Warranty Coverage)**

ပြဋ္ဌာန်းထားခြင်းမရှိပါ။

၉. ၃. စီးပွားရေးဆိုင်ရာ အချက်အလက်များကို လျှို့ဝှက်ခြင်း **(Confidentiality of Business Infromation)**

၉. ၃. ၁ လျှို့ဝှက်အချက်အလက်များအဖြစ်သတ်မှတ်ထားသော အချက်အလက်များ **(Scope of Confidential Information)**

သက်သေခံလက်မှတ်ဌာနရမ်းသုံးစွဲသူ (CA)၏ အချက်အလက်များထဲမှ အောက်ဖော်ပြပါ အချက်အလက်များကို လျှို့ဝှက်အချက်အလက်များ (Confidential and Private Information) ဟု သတ်မှတ်ပါသည်။

- CA များ၏ သက်သေခံလက်မှတ်လျှောက်ထားခြင်းဆိုင်ရာ အချက်အလက်များ (Root CA မှ လက်ခံသည်ဖြစ်စေ၊ လက်မခံသည်ဖြစ်စေ)၊
- သက်သေခံလက်မှတ်လျှောက်ထားခြင်းဆိုင်ရာ ပူးတွဲပေးပို့သော အချက်အလက်များ၊

- လုပ်ငန်းဆောင်ရွက်မှုဆိုင်ရာမှတ်တမ်းများ (မှတ်တမ်းများအပြည့်အဝအားလုံးနှင့် စာရင်းစစ်ခြင်းဆိုင်ရာ မှတ်တမ်းများ)၊
- CA များ၏ စာရင်းစစ်ခြင်းဆိုင်ရာအစီရင်ခံစာများ၊ မှတ်တမ်းများ၊
- Contingency Plan နှင့် Disaster Recovery Plan များ၊
- Hardware, Software များ၏ Operation နှင့်သက်ဆိုင်သည့် လုံခြုံရေးအစီအစဉ်များ၊ လုပ်ငန်းစီမံအုပ်ချုပ်မှုဆိုင်ရာဝန်ဆောင်မှုပေးခြင်းတို့နှင့် သက်သေခံလက်မှတ်လျှောက်ထားခြင်းတို့နှင့် ပတ်သက်သည့် အချက်အလက်များ၊

၉. ၃. ၂ လျို့ဝှက်အချက်အလက်များဟု မသတ်မှတ်ထားသော အချက်အလက်များ (Information not within the Scope of Confidential Information)

သက်သေခံလက်မှတ်များ၊ သက်သေခံလက်မှတ် ပယ်ဖျက်ခြင်းနှင့် အခြားသက်သေခံလက်မှတ်၏ အခြေအနေ (Status) ဆိုင်ရာ သတင်းအချက်အလက်များ၊ Root CA National Repository နှင့် ၎င်းအတွင်းရှိ သတင်းအချက်အလက်များကို လျို့ဝှက်နှင့် ပုဂ္ဂိုလ်ရေးရာဆိုင်ရာအချက်အလက်များ (Confidential and Private Information) များအဖြစ် မသတ်မှတ်ပါ။ ဤ CP ပါ အချက်အလက်များသည် အများပြည်သူကို ကြည့်ရှုခွင့်၊ သိရှိခွင့်ပေးထားသော အချက်အလက်(Information) Non-Confidential များဖြစ်ပါသည်။ အပိုဒ် (၉. ၃. ၁)တွင် လျို့ဝှက်အချက်အလက်များဟု သတ်မှတ်ထားသောအချက်များတွင် မပါဝင်သော အချက်အလက်များကို လျို့ဝှက်ရန်မလိုသော၊ ပုဂ္ဂလိုရေးရာဆိုင်ရာမဟုတ်သောအချက်အလက်များ (Non-Confidential (သို့) Non-Private Information) ဟု သတ်မှတ်ပါသည်။

၉. ၃. ၃ လျို့ဝှက်အချက်အလက်များကို ကာကွယ်ရန် တာဝန်ယူဆောင်ရွက်မှု (Responsibility to Protect Confidential Information)

Root CA သည် အခြားသော မသက်ဆိုင်သူများ (Third Parties) မှ လျို့ဝှက်နှင့် ပုဂ္ဂိုလ်ရေးရာဆိုင်ရာအချက်အလက် (Cconfidential/ Private Information) များကို ချိုးဖောက်ဝင်ရောက်ကြည့်ရှုခြင်းမပြုလုပ်နိုင်ရန် စီမံ ဆောင်ရွက်ထားပါသည်။

၉. ၄ တစ်ဦးတစ်ယောက်နှင့်ဆိုင်သည့်ကိုယ်ရေးအချက်အလက်များကို လုံခြုံမှုရှိအောင်ဆောင်ရွက်ခြင်း (Privacy of Personl Information)

၉. ၄. ၁ ပုဂ္ဂိုလ်ရေးရာဆိုင်ရာ အချက်အလက် လျှို့ဝှက်ခြင်းစီမံချက် (Privacy Plan)

Root CA နှင့် လက်အောက်ခံ CA များ၊ RA များသည် တစ်ဦးတစ်ယောက်နှင့်ဆိုင်သည့် ကိုယ်ရေးအချက်အလက်များကို လုံခြုံမှုရှိအောင် ဆောင်ရွက်ရန်အတွက် ညွှန်ကြားချက်များနှင့်ကိုက်ညီမှုရှိသော Privacy Policy ကို ရေးဆွဲ ဆောင်ရွက်ပါသည်။

၉. ၄. ၂ ကိုယ်ရေးလျှို့ဝှက်အဖြစ်သက်မှတ်သည့်အချက်အလက်များ (Information Treated as Private)

သက်သေခံလက်မှတ်လျှောက်ထားသူနှင့် သက်ဆိုင်သည့်အချက်အလက်များထဲမှ Root CA မှ ထုတ်ပေးသည့် သက်သေခံလက်မှတ်များ၊ သက်သေခံလက်မှတ် Directory များ၊ on line ARL/CRL တွင် ဖော်ပြသည့်အချက်အလက်များမှလွဲ၍ ကျန်သောအချက် အလက်အားလုံးကို ကိုယ်ရေးလျှို့ဝှက်အချက်များဟု သတ်မှတ်ပါသည်။

၉. ၄. ၃ ကိုယ်ရေးလျှို့ဝှက်မဟုတ်ဟုအသိအမှတ်ပြုထားသောအချက်အလက်များ (Information Not Deemed Private)

အများပြည်သူကြည့်ရှုနိုင်သည့် သက်သေခံလက်မှတ်တွင် ဖော်ပြထားသည့် အချက်အလက်များသည် ကိုယ်ရေးလျှို့ဝှက် အချက်အလက်များမဟုတ်ပါ။

၉. ၄. ၄ ကိုယ်ရေးလျှို့ဝှက်အချက်များကို ကာကွယ်ရန်တာဝန်ယူမှုများ (Responsibility to Protet Private Information)

Root CA နှင့် ၎င်း၏ Participant အားလုံးသည် လက်ခံရရှိထားသည့် လျှို့ဝှက်အချက်အလက် များကို ချိုးဖောက်ကြည့်ခံရခြင်း (Compromise) နှင့် အခြားမသက်ဆိုင်သူအဖွဲ့အစည်းများထံ ပေးပို့ခြင်း/ဖော်ပြခြင်း မဖြစ်စေရန် ကာကွယ်ရမည့်အပြင် တရားစီရင်ပိုင်ခွင့်အရ ပြည်တွင်းရှိပြဋ္ဌာန်းထားသည့် ဥပဒေများအတိုင်းလည်း ကိုက်ညီမှုရှိစေရန်ထားရှိပါသည်။

၉. ၄. ၅ ကိုယ်ရေးအချက်အလက်များကိုအသုံးပြုရန်အတွက် အကြောင်းကြားခြင်းနှင့် သဘောတူညီချက် (Notice and Consent to use Private Information)

ဤ CP တွင် ပါရှိသည့် ကိုယ်ရေးအချက်အလက်များကို သက်ဆိုင်သည့် Privacy Policy (သို့) လျှောက်ထားသူ၏ သဘောတူညီချက်မရရှိခဲ့လျှင် (လျှောက်ထားသူ၏ ခွင့်ပြုချက်မရရှိပဲ) အသုံးပြုမည်မဟုတ်ပါ။ ဤအပိုင်းသည် Privacy ဆိုင်ရာ ကာကွယ်ထားရှိရမည့် သတ်မှတ်ချက်များအတိုင်းဖြစ်ပါသည်။

၉. ၄. ၆ တရားစီရင်ရေး (သို့) စီမံခန့်ခွဲရေးဆိုင်ရာ လုပ်ငန်းစဉ်နှင့်အညီ ဖော်ပြပေးခြင်း (Disclosure Pursuant to Judicial or Administrative Process)

Root CA သည် မိမိတွင်ထားရှိသော Confidential နှင့် Private Informatin များကို တရားစီရင်ရေးဆိုင်ရာ၊ စီမံခန့်ခွဲရေးဆိုင်ရာကိစ္စများ (သို့) အခြားသောတရားရေးဆိုင်ရာဆောင်ရွက်ရန် လိုအပ်သောလုပ်ငန်းများ (Legal Process) များအတွက်သာ ကြီးကြပ်မှုအဖွဲ့၏ ခွင့်ပြုချက်ဖြင့်သာ ဖော်ထုတ်ပြသခွင့် ရှိပါသည်။

၉.၄.၇ အခြားသောအချက်အလက်များ ထုတ်ဖော်ရန်အခြေအနေများ (Other Information Disclosure Circumstances)

ဗဟိုအဖွဲ့နှင့် ကြီးကြပ်မှုအဖွဲ့တို့မှ လိုအပ်သလိုပြဋ္ဌာန်းပါသည်။

၉.၅ ဉာဏ်စွမ်းရည်ပိုင်ဆိုင်ခွင့်ဆိုင်ရာအခွင့်အရေး (Intellectual Property Right)

Root CA သည် CA များနှင့် Relying Party များအား ဉာဏ်စွမ်းရည် ပိုင်ဆိုင်ခွင့်ဆိုင်ရာ အခွင့်အရေးပေးခြင်း(IPR) (သို့) ထိုသို့ပြုလုပ်ပေးရန် အခွင့်အာဏာနှင့် တာဝန်မရှိပါ။ ဤ CP မှ ကူးယူသောမည်သည့်အကြောင်းအရာမဆို ဤ CP မှကူးယူကြောင်း၊ ကိုးကားကြောင်း ကိုးကားချက်၊ ရည်ညွှန်းချက် ပါရှိရပါမည်။

Root CA သည် အောက်ဖော်ပြပါ အကြောင်းအရာတို့နှင့် ပတ်သက်၍ မူပိုင်ခွင့်ဥပဒေအရ Root CA ၏ မူပိုင်ဟု သတ်မှတ်ပါသည်။

- Root CA ၏ Hard ware များနှင့် ရေးသားထားသော Software များ၊
- ဤ CP နှင့် CPS၊
- Root CA ၏အမည်၊
- Internet Domain name ၊
- Root CA ၏ Key pair များ။

၉.၆ ကိုယ်စားပြုမှုများနှင့် အာမခံချက်များ (Representations and Warranties)

၉.၆.၁ Root CA မှတာဝန်ယူမည့် အချက်များနှင့် အာမခံချက် (Root CA Representations and Warranties)

Root CA မှအောက်ပါအချက်များနှင့် စပ်လျဉ်း၍လုံလောက်သောသေချာမှုရှိရမည် -

-ကြီးကြပ်မှုအဖွဲ့နှင့် Root CA မှ အတည်ပြုထုတ်ပေးထားသော သက်သေခံလက်မှတ်လျှောက်လွှာများ (သို့) ထုတ်ပေးပြီးသော သက်သေခံလက်မှတ်များမှ အချက်အလက်များကို မှားယွင်းစွာ ဖော်ပြခြင်း (Misrepresentation) မရှိရပါ။

- သက်သေခံလက်မှတ်လျှောက်ထားခြင်း (Certificate Application) (သို့) သက်သေခံလက်မှတ် ပြုလုပ်ခြင်းတို့ကို စီမံဆောင်ရွက်ရာ၌ သက်သေခံလက်မှတ်မှ အချက်အလက်များ(Information) များကို သက်သေခံ လက်မှတ်လျှောက်ထားခြင်း အတည်ပြုသူ (သို့) သက်သေခံလက်မှတ် ပြုလုပ်သူ၏ သတိချို့ယွင်းမှုကြောင့် အမှားများမပါရှိစေရပါ။
- Root CA မှ ထုတ်ပေးသော သက်သေခံလက်မှတ်များသည် ဤ CP တွင်ပါရှိသော၊ လိုအပ်သော သတ်မှတ်ချက်များ အားလုံး(All Material Requirement)နှင့် ကိုက်ညီမှု ရှိပါသည်။
- Revocation Services နှင့် National Repository အသုံးပြုမှုသည် CPS များရှိ သတ်မှတ်ချက်များ (Material Aspects) အားလုံးနှင့် ကိုက်ညီမှုရှိပါသည်။

၉. ၆. ၂ CA မှတာဝန်ယူမည့် အချက်များ (CA Representation and Warranties)

CA အဖြစ်လျှောက်ထားသူမှ အာမခံရမည့်အချက်များမှာ-

- သက်သေခံလက်မှတ်တွင်ပါသည့် Public Key နှင့် ၎င်းနှင့်သက်ဆိုင်သော Private Key ကိုသုံး၍ ရေးထိုးထားသော Digital Signature တိုင်းသည် သက်သေခံလက်မှတ်ဌားရမ်းသုံးစွဲသူ(CA) ၏ Digital Signature ဖြစ်သည်။ ထို Digital Signature ကို လက်မှတ်ရေးထိုး နေချိန်တွင် ၎င်း သက်သေခံလက်မှတ်သည် အသုံးပြု၍ရသော အခြေနေတွင်ရှိပြီး သက်တမ်းကုန်ဆုံးခြင်း (Expired) (သို့) ပယ်ဖျက်ခြင်း(Revoked) လုပ်ထားခံရခြင်း အခြေအနေမျိုးမဖြစ်စေရပါ။
- ၎င်းတို့၏ Private Key ကိုသေချာစွာထိန်းသိမ်းကာကွယ် ထားရမည်။ မည်သည့် ခွင့်ပြုမထားသောသူ (Unauthorized Person) မှ သက်သေခံလက်မှတ်ဌားရမ်းသုံးစွဲသူ၏ Private Key ကိုယူ၍ သုံးစွဲနိုင်ခြင်း မရှိစေရပါ။
- သက်သေခံလက်မှတ်လျှောက်ထားရာတွင် သက်သေခံလက်မှတ်လျှောက်ထားသူမှပေးသော အချက် အလက်များသည် မှန်ကန်မှုရှိရပါမည်။
- သက်သေခံလက်မှတ်တွင် ပါဝင်သောအချက်များသည် မှန်ကန်ပါသည်။
- သက်သေခံလက်မှတ်ကို ဤ CP တွင်ပါရှိသည့် ခွင့်ပြုထားသော၊ တရားဝင်သော ဥပဒေဆိုင်ရာ ရည်ရွယ်ချက်များ (Authoriged and Legal Purose) အတွက်သာ အသုံးပြုပါမည်။

၉. ၆. ၃ Relying Party များမှတာဝန်ယူမည့်အချက်များ (Relying Party Representation and Warranties)

Relying Party များသည် မိမိယုံကြည်မှုပြုသည့် သက်သေခံလက်မှတ်သည် ယုံကြည်သင့်မသင့် စဉ်းစားဆုံးဖြတ်ရန်လိုအပ်ကြောင်း၊ Relying Party Agreement တွင် ရေးသားဖော်ပြချက်များကို နားလည်ပါကြောင်းနှင့် သက်သေခံလက်မှတ်ဆိုင်ရာအချက်အလက်၊ ၎င်းနှင့် ပါတ်သက်သောအချက်အလက်များကို ယုံကြည်စိတ်ချသင့် မသင့် ဆုံးဖြတ်ခြင်းမှာ မိမိတွင်သာတာဝန်ရှိကြောင်း နားလည်သိရှိရမည် ဖြစ်ပါသည်။

အထက်စာပိုဒ်တွင်ဖော်ပြထားသော Relying Party များ လိုက်နာဆောင်ရွက်ရမည့်တာဝန်များ (Obligation) ကို လိုက်နာမှုမရှိခြင်းကြောင့် ဥပဒေဆိုင်ရာအကျိုးဆက်များ ဖြစ်ပေါ်လာပါက ၎င်းတို့မှ ခံယူရမည်၊ လက်ခံရမည်၊ တာဝန်ယူရမည် ဖြစ်ပါသည်။

Root CA ၏ ယုံကြည်စိတ်ချစွာသုံးစွဲသူများ၏ သဘောတူညီချက် (Relying Party Agreement) တွင် အခြားသော ဖော်ပြချက်များနှင့် အာမခံချက်များကိုလည်း ထည့်သွင်းဖော်ပြထားပါသည်။

၉. ၆. ၄ အခြားသောသူများ၏ ကိုယ်စားပြုမှုနှင့် တာဝန်ယူမှုများ (Representation and Warranties of other Paticipants)

ပြဋ္ဌာန်းထားခြင်းမရှိပါ။

၉. ၇ Warranties များကို ငြင်းပယ်ခြင်း (Disclaimers of Warranties)

တည်ဆဲဥပဒေများတွင်ခွင့်ပြုထားသည့် ရည်ရွယ်ချက်များအရ သက်သေခံလက်မှတ်သုံးစွဲသူများ သဘောတူညီချက် (Subscriber Agreement) နှင့် Relying Party Agreement များသည် Root CA ၏ဖြစ်နိုင်သမျှ Warranties အားလုံးကို (Warranity of Merchantability (သို့) ရည်ရွယ်ချက် တစ်ခုအတွက် သင့်တော်မှုကို အကျုံးဝင်သောမည့် Warranty မျိုးကိုမဆို) ငြင်းပယ်နိုင်သည်။ ထို့ပြင် ပေါ့ဆမှု (Negligence) သို့မဟုတ် လက်ခံနိုင်ဖွယ်ရှိသော သတိမူခြင်းမရှိမှု (Lack of Reasonable Care) တို့အပြင် ARL/CRL တွင်ဖော်ပြထားသော ဆိုင်းငံ့၊ ပယ်ဖျက်ပြီးသား သက်သေခံလက်မှတ်များအား သုံးစွဲခြင်းကြောင့် ဖြစ်ပေါ်လာသော အကျိုးဆက်များအတွက် မည်သည့်ပေးရန်တာဝန် (Liability) ကိုမဆို Root CA မှ ငြင်းပယ်နိုင်သည်။

၉. ၈ ပေးရန်ရှိသည်များကို ကန့်သတ်ထားချက်များ (Limitations of Liability)

Root CA သည် သက်သေခံလက်မှတ်သုံးစွဲမှုကြောင့် ဖြစ်ပေါ်သည့် တိုက်ရိုက် (သို့) တိုက်ရိုက်မဟုတ်သော(Indirect), ထူးခြားသော(Special), အပြစ်ပေးခံရမှုကြောင့်ဖြစ်ပေါ်လာသော ထိခိုက်ဆုံးရှုံးမှုများ (Punitive Damage)၊ မတော်တဆ ဖြစ်သော ထိခိုက်ဆုံးရှုံးမှုများ (Incidental)

စသည်တို့ကြောင့် ဖြစ်ပေါ်သောပျက်စီးဆုံးရှုံးမှုများ ကိုလည်းကောင်း၊ စစ်ပွဲများ နှင့် သဘာဝဘေး အန္တရယ်များကြောင့် ဖြစ်ပေါ် သောပျက်စီးများအတွက်လည်းကောင်း၊ လျော်ကြေးငွေပေးခြင်း၊ မပြုလုပ်ပါ။

၉. ၉ လျော်ကြေးငွေပေးခြင်းမှ ကင်းလွတ်ခြင်း (Idemnities)

ပြဋ္ဌာန်းထားခြင်းမရှိပါ။

၉. ၁၀ စည်းကမ်းချက်များနှင့် ရပ်စဲခြင်း (Terms and Termination)

၉. ၁၀. ၁ စည်းကမ်းချက် (Term)

ဤ CP သည် Root CA ၏ National Repository တွင် Publication ပြုလုပ်သည့်နေ့မှစ၍ တရားဝင်(Effective) ပါသည်။ ဤ CP တွင် ပြင်ဆင်မှုများပြုလုပ်ပါက ထိုပြင်ဆင်မှုများသည် National Repository တွင် ထုတ်ပြန် (Publish) ပြုလုပ်သည့်နေ့မှစ၍အကျုံးဝင် သက်ရောက်မှုရှိပါသည်။

၉. ၁၀. ၂ ရပ်စဲခြင်း (Termination)

မကြာခဏ ဤ CP တွင် ပြင်ဆင်မှုများသည် Version အသစ်ပြဋ္ဌာန်းခြင်းနှင့် ပြောင်းလဲမှု ပြုလုပ်ခြင်း မပြုလုပ်သရွေ့ တရားဝင် CP ဖြစ်ပါသည်။

၉. ၁၀. ၃ ရပ်စဲခြင်းအကျိုးတရားများနှင့် လုပ်ငန်းဆက်လက်ရပ်တည်ခြင်း (Effect of Termination and Survival)

ဤ CP ကိုဖျက်သိမ်းလိုက်သော်လည်း Root CA ၏ participant များသည် certificate များ ၏ Validity Period ပြည့်သည့်တိုင်အောင် ထို CP ပါအချက်များအတိုင်း အကျုံးဝင်မှုရှိပါသည်။

၉. ၁၁ တစ်ဦးချင်းစီအားအကြောင်းကြားခြင်းနှင့် ဆက်သွယ်ခြင်း (Individual Notices and Communications with Participants)

လိုအပ်သလိုပြဋ္ဌာန်းပါသည်။

၉. ၁၂ ပြင်ဆင်မှုများ (Amendements)

၉. ၁၂. ၁ ပြင်ဆင်မှုများပြုလုပ်သည့် လုပ်ထုံးလုပ်နည်းနှင့် Specification ပြောင်းလဲမည့် လုပ်ထုံးလုပ်နည်း (Procedure for Amendment/ Specification Change Procedure)

ဤ CP တွင် ပြင်ဆင်မှုများကို Root CA Policy Management Authority မှ ပြုလုပ်ပါသည်။ ပြင်ဆင်မှုများကို ရေးသားထားသည့် Amended Form စာရွက်ပုံစံဖြင့်၄င်း၊ Update ပုံစံဖြင့်၄င်း၊ ရှိနိုင်ပါသည်။ ပြုပြင်ပြီးသား CP Version များ (သို့) notices section တွင်လည်း Link ပေးထားမည် ဖြစ်ပါသည်။ တည်ရှိသည့် URL မှာ https://www.rootca.org.mm/ repository/updates ဖြစ်ပါသည်။ Root CA ၏ စီမံအုပ်ချုပ် သူများနှင့် ကြီးကြပ်မှုအဖွဲ့မှ ဤ CP တွင်ပြောင်းလဲခြင်း ပြုလုပ်မှုများသည် CP Object Identifier များတွင်လည်း ပြောင်းလဲမှုလိုမလို ဆုံးဖြတ်ချက်ပေးပါသည်။

၉.၁၂.၂ လုပ်ထုံးလုပ်နည်းများကို ထုတ်ပြန်ခြင်းနှင့် သတိပေးအကြောင်းကြားခြင်း (Publication and Notification Procedures)

Root CA သည် CP တွင်ပါရှိသည့် စာပုံနှိပ်ခြင်းဆိုင်ရာအမှားများ၊ URL ပြောင်းလဲမှုများ၊ ဆက်သွယ်ရမည့်လိပ်စာ ပြောင်းလဲမှုများ စသည်တို့ကို ကြိုတင်အကြောင်းကြားခြင်းမရှိဘဲ ပြုပြင် ပြောင်းလဲခွင့်ရှိသည်။

၉.၁၂.၃ OID ပြောင်းလဲခြင်းပြုလုပ်မည့် အခြေအနေများ (Circumstances under which OID Must be Changed)

လိုအပ်သလိုပြဋ္ဌာန်းပါသည်။

၉.၁၃ ပြဿနာများကို ဖြေရှင်းမည့်ကျင့်ထုံးများ (Dispute Resolution Procedures)

Root CA နှင့် CA များအကြား ပဋိပက္ခများဖြစ်ပွားလာပါက ကြီးကြပ်မှုအဖွဲ့မှ သင့်လျော်သည့်နည်းဖြင့်ဖြေရှင်းပါသည်။

CA များနှင့် Subscriber များအကြား ပဋိပက္ခများဖြစ်ပွားလာပါက Root CA မှ တိုက်ရိုက် (သို့)ခုံသမာဓိလူကြီး(Arbitrator) မှတဆင့် စေ့စပ်ခြင်း(Mediate) ပြုလုပ်ခြင်းဖြင့် ဖြေရှင်းပေးရန် တာဝန်ရှိပါသည်။ သို့ဖြစ်ပါ၍ ယင်းကဲ့သို့ဖြေရှင်းနိုင်ရန် Root CA သည် ထိုသူနှစ်ဦးလုံးထံမှ အချက်အလက်နှင့် အထောက်အထား စာရွက်စာတမ်းများကို (Information and Materials) ဤ CP တွင် ဖော်ပြထားသည့်အတိုင်း တောင်းခံနိုင်ပါသည်။

အကယ်၍ ပြဿနာများကို Root CA မှ တာဝန်ယူ မဖြေရှင်းနိုင်ပါက ကြီးကြပ်မှုအဖွဲ့နှင့် ဗဟိုအဖွဲ့သို့ ဆက်လက်တင်ပြ ဖြေရှင်းဆောင်ရွက်မည်ဖြစ်ပါသည်။

၉.၁၄ လွှမ်းမိုးသည့် ဥပဒေ (Governing Law)

ဤ CP တွင် ဖွင့်ဆိုထားသည့် အတိုင်း ဘာသာပြန်ခြင်း (Interpret) ၊ တည်ဆောက်ခြင်း (Construction)၊ အာဏာတည်စေခြင်း(Enforceability) နှင့် တရားဝင်ဖြစ်ခြင်း (Validity) များနှင့်စပ်လျဉ်း၍ မြန်မာနိုင်ငံ၏ တည်ဆဲဥပဒေများအရသာ ဆောင်ရွက်ရမည် ဖြစ်ပါသည်။ မြန်မာနိုင်ငံ၏ တည်ဆဲဥပဒေများသာ လျှင် ဤ CP ကို လွှမ်းမိုးသည့် ဥပဒေဖြစ်ပါသည်။

၉. ၁၅ သက်ဆိုင်သည့်ဥပဒေများနှင့် ကိုက်ညီမှုရှိခြင်း (Compliance with Applicable Law)

ဤ CP သည် မြန်မာနိုင်ငံတော်အစိုးရ မှ ပြဋ္ဌာန်းထားသည့် ဥပဒေများ၊ သက်ဆိုင်သည့်နည်းဥပဒေများ (Regulations)၊ စည်းမျဉ်းများ (Rules)၊ အမိန့်ကြေငြာစာများ၊ ညွှန်ကြားချက်များ နှင့် ကိုက်ညီမှုရှိပါသည်။

၉. ၁၆ အထွေထွေ ကြိုတင်စီမံချက်များအပိုင်း (Miscellaneous Provisions)

၉. ၁၆. ၁ သဘောတူညီချက်အားလုံး (Entire Agreement)

မသက်ဆိုင်ပါ။

၉. ၁၆. ၂ တာဝန်နှင့် အခွင့်အရေးများ ထပ်ဆင့်ပေးအပ်ခြင်း (Assigment)

ဤ CP တွင် ပါဝင် အကျုံးဝင်သူများသည် မိမိအားပေးအပ်ထားသည့် တာဝန်နှင့် အခွင့်အရေးများကို Root CA ၏ သဘောတူ ခွင့်ပြုချက်မရဘဲ လွှဲပြောင်း ပေးအပ်ခြင်းမပြုရ။

၉. ၁၆. ၃ ဥပဒေအရဆောင်ရွက်နိုင်မှု (Serverability)

ဤ CP ပါဖော်ပြချက် (သို့မဟုတ်) ပြဋ္ဌာန်းချက်၊ စည်းကမ်းချက်တစ်ခုနှင့် စပ်လျဉ်း၍ ပေါ်ပေါက်လာသည့် အခြေအနေတစ်ရပ်တွင် တရားရုံးတော် (Court of Law) (သို့) အခြားသော ခုံရုံးများတွင် တင်ပြကိုးကားခြင်း မပြုနိုင်ခဲ့သော်လည်း ထိုဖော်ပြချက် (သို့မဟုတ်) စည်းကမ်းချက်မှလွဲ၍ ÞCP ၏ ကျန်အစိတ်အပိုင်းများသည် ဥပဒေအရ ဆက်လက်၍ အကျိုးသက်ရောက်မှုရှိ (Valid) ပါသည်။

၉. ၁၆. ၄ အာဏာသက်ရောက်ခြင်း(ကိုယ်စားလှယ်၊ရှေ့နေအကျိုးဆောင်ခနှင့်စွန့်လွှတ်သူ၏ အခွင့်အရေး) Enforcement (Attorney's Fees and Waiver of Rights)

မသက်ဆိုင်ပါ။

၉. ၁၆. ၅ မတားဆီးနိုင်သော၊ မလွန်ဆန်နိုင်သောဖြစ်ရပ် (Force Majeure)

Root CA သည် သဘာဝဘေးအန္တရာယ်များ၊ စစ်ဘေး စသည့် တားဆီး၍ မရနိုင်သော ကိစ္စရပ်များကြောင့် ဖြစ်ပေါ်လာသော ပျက်စီးဆုံးရှုံးမှုများအတွက် ပေးလျော်ရန်တာဝန်မရှိပါ။

၉. ၁၇ အခြားသောကြိုတင်စီမံချက်များ (Other Provisions)

လိုအပ်သလို ပြဋ္ဌာန်းပါသည်။

၉. ၁၈ မှတ်ချက်များပေးပို့ ရန်ကာလ (Comment Period)

ဤ CP နှင့်စပ်လျဉ်း၍ အကြံပြုချက်၊ မှတ်ချက်များ ပေးပို့လိုပါက ဤ CP အား publish လုပ်သည့်နေ့မှစ၍ (၁၅)ရက်အတွင်း Root CA သို့ အကြောင်းကြားစာပေးပို့ နိုင်ပါသည်။

နောက်ဆက်တွဲ (က)

အတိုကောက်စကားလုံးများနှင့်အဓိပ္ပယ်ဖွင့်ဆိုချက်ဇယားများ

Table of Acronyms

ဝေါဟာရ	အဓိပ္ပယ်သတ်မှတ်ချက်
ARL	Authority Revocation List
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
FIPS	အမေရိကန်ပြည်ထောင်စု Federal Information Processing Standards
CA	Certification Authority
LDAP	Light Weight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PKCS	Public-Key Cryptography Standard
PKI	Public-Key Infrastrature
Root CA	Root Certificatioin Authority
RA	Registration Authority
RFC	Request For Comment
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer

<u>နောက်ဆက်တွဲ (ခ)</u>

<u>အဓိပ္ပါယ်သတ်မှတ်ချက်</u>

(က) **သက်သေခံလက်မှတ် (Certificate)** ဆိုသည်မှာ လက်မှတ်ရေးထိုးသူနှင့် ထိုးမြဲလက်မှတ် ဖန်တီးသော အချက်အလက်တို့၏ ဆက်နွယ်မှုကို သေချာစေသည့် အီလက်ထရောနစ် အချက်အလက်သတင်းလွှာ

သို့မဟုတ် အခြားမှတ်တမ်းအဖြစ် သက်သေခံလက်မှတ်ထုတ်ပေးသူက ငှားရမ်းသုံးစွဲသူ (Subscriber) အား ထုတ်ပေးသည့်လက်မှတ်ကိုဆိုလိုသည်။

(သို့မဟုတ်)

သက်သေခံလက်မှတ် (Certificate) ဆိုသည်မှာ သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ (CA) ၏ private key ဖြင့် ရေးထိုးထားသော ဒစ်ဂျစ်တယ်ထိုးမြဲလက်မှတ် (digital signature) ဖြင့် ထုတ်ပေးထားသော သက်သေခံလက်မှတ် ငှားရမ်းသုံးစွဲသူ (end entity) ၏ public key နှင့် အခြားသောအချက်အလက်များ ပါဝင်သည့် အချက်အလက်ဖွဲ့စည်းမှု (data structure) ကိုဆိုလိုသည်။

(ခ) **မူလအရင်းအမြစ်သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ (Root Certification Authority)** မူလအရင်းအမြစ်သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ (**Root Certificate Authority)** သည် သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ(CA) များသို့ သက်သေခံလက်မှတ်များ ထုတ်ပေးခြင်း ၊ စီမံခန့်ခွဲခြင်း၊ ပယ်ဖျက်ခြင်း၊ သက်တမ်းတိုးခြင်းများပြုလုပ်နိုင်ရန် အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေးဥပဒေအရ ကြီးကြပ်မှုအဖွဲ့က အမိန့်စာဖြင့် တာဝန်ပေး ခန့်အပ်ထားသော အဖွဲ့အစည်း ဖြစ်ပါသည်။

(ဂ) **သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ (Certificate Authority (CA))** ဆိုသည်မှာ အီလက်ထရောနစ် ထိုးမြဲလက်မှတ်နှင့် စပ်လျဉ်း၍ ဝန်ဆောင်မှုလုပ်ငန်း ဆောင်ရွက်နိုင်ရန် ကြီးကြပ်မှုအဖွဲ့က အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေးဥပဒေအရ ထုတ်ပေးသည့်လိုင်စင်ကို ရရှိသောပုဂ္ဂိုလ် သို့မဟုတ် အဖွဲ့အစည်းကိုဆိုလိုသည်။

(သို့မဟုတ်)

သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ (Certificate Authority (CA))

CA လုပ်ပိုင်ခွင့် လိုင်စင်ရရှိထားသူ (**CA**)များသည် Root CA မှထုတ်ပေးသော သက်သေခံလက်မှတ်များကို ငှားရမ်းသုံးစွဲသူများ ဖြစ်ပါသည်။ CA များသည် တစ်ဦးချင်း သော်လည်းကောင်း၊ အဖွဲ့အစည်းသော်လည်းကောင်း ဖြစ်နိုင်ပါသည်။

(ဃ) **သက်သေခံလက်မှတ်ပေါ်လစီ (Certifice Policy (CP))** ဆိုသည်မှာ သာမန်လုံခြုံမှုလိုအပ်ချက်များ နှင့်အညီ အဖွဲ့အစည်းတစ်ခု သို့မဟုတ် အသုံးချမှု အဆင့်အတန်းတစ်ခု အတွက် သက်သေခံ လက်မှတ်တစ်ခု အသုံးပြုနိုင်မှုကို ဖော်ပြသော နည်းဥပဒေ အစုအဖွဲ့ကို ဆိုလိုသည်။

(၄) **သက်သေခံလက်မှတ်ထုတ်ပေးခြင်းဆိုင်ရာ လိုက်နာကျင့်သုံးရမည့်နည်းလမ်းများ (Certification Practice Statement (CPS))** ဆိုသည်မှာ သက်သေခံလက်မှတ်များထုတ်ပေးရာတွင် သက်သေခံလက်မှတ် ထုတ်ပေးပိုင်ခွင့်ရှိသူ (CA) မှ အသုံးပြုသည့် လိုက်နာကျင့်သုံးရမည့်နည်းလမ်းများ ဖော်ပြချက်ဖြစ်သည်။

(၅) **သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူပယ်ဖျက်စာရင်း (Authority Revocation List (ARL))** ဆိုသည်မှာ မူလအရင်းအမြစ်သက်သေခံလက်မှတ်ထုတ်ပေးပိုင်ခွင့်ရှိသူ (Root CA) မှ လက်မှတ်ရေးထိုး၍ အမျိုးသားသက်သေခံလက်မှတ်မှတ်တမ်းတိုက် (National Repository) တွင် အများပြည်သူ အလွယ်တကူနှင့် အခမဲ့ကြည့်ရှုနိုင်ရန် ပယ်ဖျက်ပြီးသော သက်သေခံလက်မှတ်များကို ဖော်ပြသည့် အချိန် ဆိုင်ရာ မှတ်တမ်းတင်ခြင်း (time stamp) ပြုလုပ်ထားသည့် စာရင်းတစ်ခုကို ဆိုလိုသည်။

(၆) **သက်သေခံလက်မှတ်ပယ်ဖျက်စာရင်း (Certificate Revocation List (CRL))** ဆိုသည်မှာ သက်သေခံလက်မှတ် ထုတ်ပေးပိုင်ခွင့်ရှိသူ (CA) မှ လက်မှတ်ရေးထိုး၍ သက်သေခံလက်မှတ် မှတ်တမ်းတိုက် (repository) တွင် အများပြည်သူအလွယ်တကူနှင့်အခမဲ့ကြည့်ရှုနိုင်ရန် ပယ်ဖျက်ပြီးသော သက်သေခံလက်မှတ်များကို ဖော်ပြသည့် အချိန်ဆိုင်ရာမှတ်တမ်းတင်ခြင်း (time stamp) ပြုလုပ်ထားသည့် စာရင်းတစ်ခုကို ဆိုလိုသည်။

(၇) မှတ်ပုံတင်ခွင့်လုပ်ပေးပိုင်ခွင့်ရှိသူ (RA) ဆိုသည်မှာ သက်သေခံ လက်မှတ် လျှောက်ထားသူ၏ အကြောင်းအရာများနှင့် ပတ်သက်၍ လက်ခံဆောင်ရွက် မှတ်တမ်းတင်ခြင်း(Registration)၊ လျှောက်ထားသူ အမှန်အကန် ဟုတ်မဟုတ်စစ်ဆေးခြင်း (Identification) နှင့် သက်သေခံမှုစစ်ဆေးခြင်း (Authentication) တို့အတွက် တာဝန်ယူ ဆောင်ရွက်ပေးသော လူပုဂ္ဂိုလ်(သို့မဟုတ်) အဖွဲ့အစည်းတစ်ခု ဖြစ်ပါသည်။ (ဆိုလိုသည်မှာ RA တစ်ဦးသည် CA ကိုယ်စား မှန်ကန်မှု ရှိ၊ မရှိစစ်ဆေးခြင်း(Identification) နှင့် သက်သေခံမှုစစ်ဆေးခြင်း (Authentication) တာဝန်များကို ဆောင်ရွက်ပေးပါသည်။)

(၈) **ယုံကြည်စိတ်ချစွာသုံးစွဲသူ (Relying Party)** ဆိုသည်မှာ သက်သေခံလက်မှတ်ကိုအသုံးပြု၍ သက်သေခံလက်မှတ်နှင့် ဒစ်ဂျစ်တယ်ထိုးမြဲလက်မှတ်များကို ယုံကြည်စိတ်ချစွာသုံးစွဲသူကို ဆိုလိုသည်။ ဤစာတမ်းတွင် သက်သေခံလက်မှတ်သုံးစွဲသူ (certificate user) နှင့် ယုံကြည်စိတ်ချစွာသုံးစွဲသူ (relying party) ကို အပြန်အလှန်အသုံးပြုနိုင်သည်။

(ည) **သက်သေခံလက်မှတ်လျှောက်ထားသူ (End Entity)** ဆိုသည်မှာ သက်သေခံလက်မှတ် ထုတ်ပေးပိုင်ခွင့်ရှိသူ (CA) ထံမှ သက်သေခံလက်မှတ်တစ်ခုကို တောင်းဆိုသူဖြစ်သည်။

(ဋ) **သက်သေခံလက်မှတ်သက်တမ်းတိုးခြင်း (Certificate Renewal)** ဆိုသည်မှာ သက်သေခံလက်မှတ်တွင် ပါဝင်သော public key သို့မဟုတ် တခြား အချက်အလက်များကို ပြောင်းလဲခြင်းမရှိဘဲ ငှားရမ်းသုံးစွဲသူ CA အား သက်သေခံလက်မှတ်အသစ်တစ်ခုထုတ်ပေးခြင်းဖြစ်သည်။

(ဌ) **Key pair အသစ်ကိုအသုံးပြု၍ သက်သေခံလက်မှတ်သက်တမ်းတိုးခြင်း (Certificate Rekey)** ဆိုသည်မှာ public key အသစ်တစ်ခုကိုအသုံးပြု၍ သက်သေခံလက်မှတ်ထုတ်ပေးရန်အတွက် လျှောက်ထားခြင်းဖြစ်သည်။ Certificate Re-Key သည် Public Key အသစ်တစ်ခုကို အသုံးပြု၍ သက်သေခံလက်မှတ်ထုတ်ပေးခြင်းဖြစ်ပါသည်။