Бүлэг 6а

“ТРИДУМ КЕЙ” ГЭРЧИЛГЭЭЖҮҮЛЭХ БАЙГУУЛЛАГА

Гэрчилгээжүүлэх Бодлого, Гэрчилгээжүүлэх Ажиллагааны Журам (CP/CPS)

Тридум Е-Секъюрити ХХК

АГУУЛГА

Товчилсон үгс

ХХМТГ	Харилцаа Холбоо Мэдээллийн Технологийн газар
МҮҮСГБ	Монгол Улсын Үндэсний Суурь Гэрчилгээжүүлэх Байгууллага
ГБ	Тусгай зөвшөөрөл эзэмшигч Гэрчилгээжүүлэх Байгууллага
Offline CA	Сүлжээнд холболтгүй CA
БН	Бүртгэлийн Нэгж
HSM	Hardware Security Module (техник хангамж дээр суурилсан нууцлалын төхөөрөмж)
LDAP	Lightweight Directory Access Protocol
Тоон гарын үсэг	Цахим баримт бичгийг хуурамчаар үйлдэх, өөрчлөхөөс хамгаалах зорилгоор тоон гарын үсгийн хувийн түлхүүр ашиглан мэдээллийг криптограф хувиргалтад оруулж үүсгэсэн, уг баримт бичгийн бүрдэл болох цахим гарын үсгийн төрлийг
Криптограф	Мэдээллийг нуух аргачлалыг судалдаг математикийн салбар шинжлэх ухааныг
Цахим баримт бичиг	Мэдээллийн технологийн техник хэрэгсэл, програм хангамж ашиглан үүсгэх, илгээх, хүлээн авах, хадгалах боломжтой цахим

	өгөгдлийг
Тоон гарын үсгийн хувийн түлхүүр	Тоон гарын үсгийг үүсгэх, өгөгдлийг тайлах зориулалттай тэмдэгтийн давтагдашгүй дарааллыг
Тоон гарын үсгийн нийтийн түлхүүр	Тухайн тоон гарын үсгийн хувийн түлхүүртэй математик хамааралтай, өгөгдлийг нууцлах, тоон гарын үсгийг шалгах зориулалттай тэмдэгтийн дарааллыг
Тоон гарын үсэг эзэмшигч	Тоон гарын үсгийн гэрчилгээнд заасан тоон гарын үсгийн нийтийн түлхүүр эзэмшигч иргэн, хуулийн этгээдийг
Тоон гарын үсгийн гэрчилгээ	Тоон гарын үсгийн гэрчилгээ олгох үйл ажиллагаа эрхлэх тусгай зөвшөөрөл эзэмшигчийн олгосон тоон гарын үсэг эзэмших эрх, тоон гарын үсгийн нийтийн түлхүүр, холбогдох бусад мэдээллийг агуулсан, баталгаажуулсан цахим баримт бичгийг
PKI-нийтийн түлхүүрийн дэд бүтэц	Тоон гарын үсгийн хувийн болон нийтийн түлхүүрийг үүсгэх, зохион байгуулах, хуваарилах, хэрэглэх, хадгалах болон хүчингүй болгох, түүнийг цахим харилцаанд нэвтрүүлж ашиглахтай холбогдсон тогтолцоог
Тоон гарын үсгийн хэрэгсэл	Тоон гарын үсгийн хувийн түлхүүр ашиглан цахим баримт бичгийн тоон гарын үсгийг үүсгэх, эсхүл тоон гарын үсгийн нийтийн түлхүүр ашиглан цахим баримт бичгийн бүрдэл хэсэг болох тоон гарын үсгийг шалгах, эсхүл тоон гарын үсгийн нийтийн болон хувийн түлхүүрийг үүсгэх боломж олгож байгаа техник хэрэгсэл, програм хангамжийг
Гэрчилгээжүүлэх бодлого	Гэрчилгээний нэр төрөл, зохион байгуулалт, гэрчилгээ олгох байгууллагын хүлээх үүрэг, хариуцлага, төлбөр, хураамж, нууцлал, аудит, бүртгэлийн талаар баримтлах үндсэн чиглэлийг тодорхойлсон баримт бичгийг
Гэрчилгээжүүлэх ажиллагааны	Тоон гарын үсгийн гэрчилгээ олгох үйл ажиллагаа эрхлэх тусгай зөвшөөрөл эзэмшигчийн үйл ажиллагаанд тавих шаардлага, үйл ажиллагааны үндсэн дэг, аюулгүй байдлын хяналтыг

журам (ГҮАЖ)	тодорхойлсон баримт бичгийг
CRL (ХГЖ)	Certificate Revocation List (хүчингүй гэрчилгээнүүдийн жагсаалт)
ОУСБ	Олон Улсын Стандартын Байгууллага
ГГҮЗХ (CSR)	Гэрчилгээнд Гарын Үсэг Зурах Хүсэлт (certificate signing request)
ТҮЦ машин	Төрийн Үйлчилгээний Цахим машин
ОГТП (OSCP)	Онлайн Гэрчилгээний Төлвийн Протокол (online certificate status protocol)

1. Удиртгал

1.1 Оршил

- Монгол улсын хэмжээнд нийтийн түлхүүрийн дэд бүтцийн үйлчилгээг хийх зорилготой ба “Цахим гарын үсгийн тухай” хуулийн дагуу хийгдсэн.
- Энэхүү баримт бичиг нь RFC3647 баримтын дагуу хийгдсэн.
- Энэ RFC3647 баримтын бүх бүлгүүдийг ашиглаагүй болно. Ашиглаагүй бүлэг ба дэд бүлгүүдийг "Нөхцөл байхгүй" гэж тэмдэглэсэн болно.
- Нийтийн түлхүүрийн дэд бүтцийн тоон гарын үсгийн үйлчилгээг үзүүлэх үйл ажиллагааны дүрэм ба процессийн цогц илэрхийллийг энэ баримт бичиг илэрхийлнэ.
- Уг баримт бичиг нь бодлогын болон үйл ажиллагааны журмыг агуулна.
- Тоон гарын үсгийн гэрчилгээ олгох байгууллага нь таних, аюулгүйгээр мэдээллийг дамжуулах болон тоон гэрчилгээний үйлчилгээний үйл ажиллагааг хийнэ.
- “Тридум Кей” нь энэхүү бичиг баримтад гэрчилгээ олгох байгууллагын эрхийг эдэлнэ.

1.1.1 Гэрчилгээний төрлүүд

Гэрчилгээг олгогч нь доорх төрлийн гэрчилгээнүүдийг хувь хүн болон байгууллагад үүсгэнэ.

Хувь хүнд доорх төрлийн гэрчилгээг олгоно:

- ✓ Тоон гарын үсэг зурах
- ✓ Мэдээлэл нууцлах
- ✓ Таньж нэвтрэх

Байгууллагад доорх төрлийн гэрчилгээг олгоно:

- ✓ Тоон гарын үсэг зурах
- ✓ Мэдээлэл нууцлах
- ✓ Таньж нэвтрэх
- ✓ SSL/TLS холболт үүсгэх
- ✓ Код/Агуулга баталгаажуулах

1.2 Баримт бичгийн нэр ба тодорхойлолт

Баримт бичгийн гарчиг: **Гэрчилгээжүүлэх бодлого, гэрчилгээжүүлэх үйл ажиллагаан журам**

Баримт бичгийн хувилбар : **1.0**

Баримт бичгийг үүсгэсэн огноо : **2017- 12-01**

Хүчин төгөлдөр хэрэгжиж эхлэх хугацаа: **Тусгай зөвшөөрөлд заана**

Шинэчлэх хугацаа: **Дараагийн хувилбар хүртэл**

Байгууллагыг таних код (OID) нь доорх зохион байгуулалттай байна:
Хүснэгт 1.1 OID

OID	Обьект
xxx.xxx.xxx	Гэрчилгээ олгох байгууллагын удирдлага
xxx.xxx.xxx	Гэрчилгээжүүлэх байгууллага
xxx.xxx.xxx	Гэрчилгээжүүлэх үйл ажиллагааны журам
xxx.xxx.xxx	Гэрчилгээжүүлэх бодлого
xxx.xxx.xxx	Серверийн гэрчилгээний бодлого
xxx.xxx.xxx	Харилцагчийн гэрчилгээний бодлого

1.3 Нийтийн түлхүүрийн дэд бүтцэд оролцогчид

Гэрчилгээ олгох байгууллага нь сүлжээний хэрэглэгчид ба дэд бүтэц, засгийн газрын онлайн үйлчилгээг авах, банк санхүүгийн салбарт санхүүгийн үйлчилгээг авах, үүрэн холбооны хэрэглэгчдийн үйл ажиллагаанд баталгаажуулах үйлчилгээг гүйцэтгэх, сүлжээний үйл ажиллагаанд оролцогчид байх ба уг бүлгийг гэрчилгээгээр хангана. Мөн түүнчлэн Монгол Улсын Үндэсний Гэрчилгээжүүлэх Байгууллага байна.

1.3.1 Гэрчилгээжүүлэх байгууллага

Өөрийн харъяаллын хүрээнд Гэрчилгээ олгох дэд байгууллагад зориулж гэрчилгээ үүсгэж болно.

1.3.2 Бүртгэлийн нэгж

Гэрчилгээ олгох байгууллага нь бүртгэлийн нэгжийн үйл ажиллагааг удирдан зохион байгуулна. Шаардлагатай бол нэмэлт бүртгэлийн нэгжүүдийг байгуулж болно. Гэрчилгээжүүлэх байгууллага нь бүртгэлийн нэгжтэй нууцлалтай гэрээг байгуулах уг гэрээнд аливаа бүх нөхцөлийг нарийвчлан тусгасан байна.

1.3.3 Захиалагч

Энэхүү нийтийн түлхүүрийн дэд бүтцийн үйлчилгээг авч буй оролцогч (хүмүүс, техник, програм хангамж) нь гэрчилгээ олгох байгууллагын үйл ажиллагаанд хамрагдана. Практикт, энэхүү үйл ажиллагаанд нэгдсэн компьютерийн систем болон ажилчид байдаг.

1.3.4 Итгэлцлийн талууд

Гэрчилгээ олгох байгууллагаас олгосон гэрчилгээнд тусгагдсан нийтийн түлхүүрийг тоон гарын үсгийг шалгах болон шифрлэхэд ашиглаж буй хэрэглэгчдийг итгэлцлийн талууд гэнэ..

1.3.5 Бусад оролцогч талууд

Нөхцөл байхгүй

1.4 Гэрчилгээг хэрэглэх

1.4.1 Гэрчилгээг зөв, зохистой хэрэглэх

Гэрчилгээ олгох байгууллагаас бий болгосон гэрчилгээнүүд нь X.509 гэрчилгээний стандарттай нийцсэн хэрэглээнд ашиглагдаж болно. Тухайлбал (1.1.1-т заасан) баримт бичигт тоон гарыг үсэг зурах, харилцаа холбоог баталгаажуулах болон шифрлэх, хэрэглэгчдийг таних ба бусад үйлчилгээнүүдэд.

1.4.2 Гэрчилгээг ашиглахыг хориглох нөхцөл

Гэрчилгээг зөвхөн Монгол Улсын Цахим гарын үсгийн тухай хуулийн хүрээнд хэрэглэхийг зөвшөөрнө. Монгол Улсын Цахим гарын үсгийн гэрчилгээ нь эрчим хүчний, агаарын хөлгийн навигацийн эсвэл онц чухал харилцаа холбооны зэрэг алдаа, тасалдалгүй ажиллах шаардлагатай дэд бүтэц эсвэл системд ашиглах зориулалтгүй. Дээрх төрлийн систем, дэд бүтцэд гэрчилгээг ашигласны улмаас гарч болох аливаа осол, гэмтэл, хүний амь эрстэх эсвэл байгаль орчны хохиролд Монгол Улсын Цахим гарын үсгийн тухай хуулийн хүрээнд үйл ажиллагаа явуулж буй этгээд хариуцлага хүлээхгүй.

Мөн Монгол Улсын холбогдох хуулийн дагуу хууль бус гэж үзэх мэдээлэл, цахим баримт бичгийг баталгаажуулах болон нууцлахад тоон гарын үсгийн гэрчилгээ болон холбогдох түлхүүрүүдийг ашиглахгүй.

1.5 Удирдлагын бодлого

1.5.1 Удирдлагын үүрэг

Гэрчилгээ олгох байгууллагын удирдлага нь гэрчилгээний бодлого ба үйл ажиллагааны журамд тайлбар хийх, сайжруулах болон шинэ хувилбарыг бүртгэх үүргийг гүйцэтгэнэ.

1.5.2 Холбоо барих хүн

Л.Аюушжав

Тридум Кей гэрчилгээжүүлэх байгууллага

Баянгол дүүрэг 3-р хороо
Замчдын гудамж 2
Д блок 17/2
Тел/Факс: +976-70120072
Эмайл:ca@tridumkey.mn

1.5.3 Гэрчилгээний үйл ажиллагааны журам нь бодлогын баримт бичигтэй зохицож буй эсэхийг тогтоох хүн

Гэрчилгээ олгох байгууллагын менежер нь гэрчилгээний үйл ажиллагааны журам нь бодлогын баримт бичигтэй зохицож буй эсэхийг тогтоох ажлыг хийж гүйцэтгэнэ.

1.5.4 Гэрчилгээний үйл ажиллагааны журмыг баталгаажуулах процесс

Гэрчилгээ олгох байгууллагын удирдлагын шийдвэрийг байгууллагын Гэрчилгээний Бодлогын Удирдлагын Зөвлөл (ГБУЗ) гаргах ба энэхүү зөвлөл нь тухайн байгууллагыг төлөөлнө.

Удирдлагын Зөвлөл нь доорх үүргүүдийг хүлээнэ:

- Шинэчлэгдсэн Гэрчилгээний бодлого ба гэрчилгээний үйл ажиллагааны журмыг батлах,
- Гэрчилгээ олгох байгууллагын хувийн түлхүүр алдагдсан тохиолдолд эсрэг арга хэмжээ авах,
- Гэнэтийн ослын үед яаралтай тусламжийн үйл ажиллагааг явуулах,
- Бусад чухал асуудлууд.

1.6 Тодорхойлолт ба товчилсон үг

RFC 2119 стандартад тайлбарлагдсан доорх түлхүүр үгнүүдийг энэ баримт бичигт ашиглана. “ЗАЙЛШГҮЙ” , “ЗАЙЛШГҮЙ БУС” , “ШААРДЛАГАТАЙ” , “БОЛНО” , “БОЛОХГҮЙ” , “ЁСТОЙ” , “ЁСГҮЙ” , “ЗӨВЛҮҮШТЭЙ” , “БАЙЖ БОЛОХ” , ба “БОЛОМЖИТ”

1.6.1 Нэр томьёоны тодорхойлолт

1.6.1.1 “Нийтийн түлхүүрийн дэд бүтэц” гэж тоон гарын үсгийн хувийн болон нийтийн түлхүүрийг үүсгэх, зохион байгуулах, хуваарилах, хэрэглэх, хадгалах болон хүчингүй болгох, түүнийг цахим харилцаанд нэвтрүүлж ашиглахтай холбогдсон тогтолцоог;

1.6.1.2 “Тоон гарын үсэг” гэж цахим баримт бичгийг хуурамчаар үйлдэх, өөрчлөхөөс хамгаалах зорилгоор тоон гарын үсгийн хувийн түлхүүр ашиглан мэдээллийг криптограф хувиргалтад оруулж үүсгэсэн, уг баримт бичгийн бүрдэл болох цахим гарын үсгийн төрлийг;

1.6.1.3 “тоон гарын үсгийн хувийн түлхүүр” гэж тоон гарын үсгийг үүсгэх, өгөгдлийг тайлах зориулалттай тэмдэгтийн давтагдашгүй дарааллыг;

1.6.1.4 “тоон гарын үсгийн нийтийн түлхүүр /цаашид “нийтийн түлхүүр” гэх/” гэж тухайн тоон гарын үсгийн хувийн түлхүүртэй математик

хамааралтай, өгөгдлийг нууцлах, тоон гарын үсгийг шалгах зориулалттай тэмдэгтийн дарааллыг;

1.6.1.5 “тоон гарын үсгийн хэрэгсэл” гэж тоон гарын үсгийн хувийн түлхүүр ашиглан цахим баримт бичгийн тоон гарын үсгийг үүсгэх, эсхүл тоон гарын үсгийн нийтийн түлхүүр ашиглан цахим баримт бичгийн бүрдэл хэсэг болох тоон гарын үсгийг шалгах, эсхүл тоон гарын үсгийн нийтийн болон хувийн түлхүүрийг үүсгэх боломж олгож байгаа техник хэрэгсэл, програм хангамжийг;

1.6.1.6 “тоон гарын үсгийн гэрчилгээ” гэж тоон гарын үсгийн гэрчилгээ олгох үйл ажиллагаа эрхлэх тусгай зөвшөөрөл эзэмшигчийн олгосон тоон гарын үсэг эзэмших эрх, тоон гарын үсгийн нийтийн түлхүүр, холбогдох бусад мэдээллийг агуулсан, баталгаажуулсан цахим баримт бичгийг;

1.6.1.7 “Монгол Улсын Үндэсний Суурь Гэрчилгээжүүлэх Байгууллага” гэж (Mongolian national root CA - МҮҮСГБ) – Харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны байгууллагын дэргэд байгуулагдаж, зохих дэд бүтцээр хангагдсан, тоон гарын үсгийн гэрчилгээ олгох үйл ажиллагаа эрхлэх байгууллагын нийтийн түлхүүрийг гэрчилгээжүүлэх, анхдагч бөгөөд өөрийгөө баталгаажуулах эрх бүхий цорын ганц гэрчилгээжүүлэх байгууллагыг;

1.6.1.8 “Тоон гэрчилгээний үндэсний сан” (ТГҮС - National Repository of Digital Certificates) – “Цахим Гарын Үсгийн Тухай” хуулийн дагуу олгосон бүх тоон гэрчилгээг хадгалах санг;

1.6.1.9 “Эрх бүхий байгууллага” гэж “Цахим Гарын Үсгийн Тухай” хуулийн дагуу гэрчилгээ олгох үйл ажиллагаа эрхлэх байгууллагад тусгай зөвшөөрөл олгодог, хянадаг Харилцаа Холбооны Асуудал Эрхэлсэн Төрийн Захиргааны Байгууллагыг;

1.6.1.10 ”Гэрчилгээ олгох үйл ажиллагаа эрхлэх байгууллага” (цаашид “тусгай зөвшөөрөл эзэмшигч” гэх) гэж тоон гарын үсгийн түлхүүрийн гэрчилгээ, бусад тоон гэрчилгээ үүсгэх, олгох болон хуулинд заасан бусад чиг үүргийг гүйцэтгэдэг, тоон гарын үсгийн гэрчилгээ олгох үйл ажиллагаа эрхлэх тусгай зөвшөөрөл эзэмшиж буй хуулийн этгээд;

1.6.1.11 “Гэрчилгээжүүлэх байгууллагын тоон гарын үсгийн гэрчилгээ” гэж гэрчилгээ олгох суурь байгууллагаас тусгай зөвшөөрөл эзэмшигч, түүний эрх бүхий албан тушаалтанд үүсгэж өгсөн тоон гарын үсгийн өндөр төвшний гэрчилгээг (цаашид “суурь гэрчилгээ” гэх);

1.6.1.12 “Тоон гарын үсгийн гэрчилгээ эзэмшигч” гэж “Цахим гарын үсгийн тухай” хууль, тусгай зөвшөөрөл эзэмшигчийн гэрчилгээжүүлэх бодлого, гэрчилгээ олгох журмын дагуу олгосон тоон гарын үсгийн түлхүүрийн гэрчилгээ эзэмшигч этгээдийг;

1.6.1.13 “Тусгай зөвшөөрөл эзэмшигчийн хэрэгсэл” гэж тоон гарын үсгийн гэрчилгээ, бусад тоон гэрчилгээ үүсгэх, олгох чиг үүргийг хэрэгжүүлэхэд ашиглаж буй програм болон техник хангамжийн багцыг;

1.6.1.14 “Тусгай зөвшөөрөл эзэмшигчийн гэрчилгээжүүлэх бодлого” гэж гэрчилгээний нэр төрөл, зохион байгуулалт, гэрчилгээ олгох байгууллагын хүлээх үүрэг, хариуцлага, төлбөр, хураамж, нууцлал,

аудит, бүртгэлийн талаар баримтлах үндсэн чиглэлийг тодорхойлсон баримт бичгийг;

1.6.1.15 “Тусгай зөвшөөрөл эзэмшигчийн гэрчилгээжүүлэх ажиллагааны журам” гэж тоон гарын үсгийн гэрчилгээ олгох үйл ажиллагаа эрхлэх тусгай зөвшөөрөл эзэмшигчийн үйл ажиллагаанд тавих шаардлага, үйл ажиллагааны үндсэн дэг, аюулгүй байдлын хяналтыг тодорхойлсон баримт бичгийг;

1.6.1.16 “цахим харилцаанд оролцогч” гэж цахим хэлбэрээр мэдээлэл солилцож буй төр, нутгийн удирдлагын байгууллага, хувийн хэвшлийн байгууллага, аж ахуйн нэгж, иргэдийг;

1.6.1.17 “Гэрчилгээнд гарын үсэг зурах хүсэлт” (CSR) гэж гэрчилгээ олгох төвийн хувийн түлхүүрийг агуулсан, сүлжээнд холбогдоогүй компьютерт суулгагдсан, зөвхөн уг компьютерт гэрчилгээг үүсгэн гарын үсэг зурах зорилготой мэдээллийг;

1.6.1.18 “Мэдээллийн сан” гэж гэрчилгээ олгох байгууллагын ажил үүрэгтэй холбоотой бүх мэдээллийг онлайн хадгалалт, хандалт бүхий компьютер, серверийг;

1.6.1.19 “харилцан баталгаажуулалт” гэж гадаадын болон дотоодын гэрчилгээ олгох байгууллагууд тоон гарын үсгийн гэрчилгээг харилцан баталгаажуулж хүлээн зөвшөөрөхийг;

1.6.1.20 “ITU-T X.509” гэж “Олон улсын цахилгаан холбооны байгууллага”-ын стандартчиллын хэлтсээс гаргасан нийтийн түлхүүрийн дэд бүтцийн бодлоготой холбоотой стандартыг.

1.6.1.21 “IETF RFC 3647” гэж “Интернэтийн инженерчлэлийн мэргэшсэн баг”-ийн гишүүдээс 2003 оны 11-р сард боловсруулсан нийтийн түлхүүрийн дэд бүтцийн бодлогын болон гэрчилгээжүүлэлтийн аргачлалыг.

1.6.1.22 Хүчингүй Гэрчилгээний Жагсаалт (Certificate Revocation List) гэж гэрчилгээг хүчингүй болгосон, түдгэлзүүлсэн тухай мэдээллийг агуулсан мэдээллийн санг

2. Хэвлэн нийтлэх болон хадгалах байрны үүрэг

2.1 Хадгалах байрнууд

Гэрчилгээ олгох байгууллагын мэдээллийг олж авах онлайн хадгалах газар нь https://www.tridumkey.mn байна.

2.2 Гэрчилгээний мэдээллийг хэвлэн нийтлэх

Гэрчилгээ олгох байгууллага нь олон нийт хандах зориулалт бүхий веб серверийн үйлчилгээг хийх ба веб сервер нь доорх зүйлсийг агуулсан байна:

- Гэрчилгээ олгох байгууллагын гэрчилгээ болон гэрчилгээний хүчин төгөлдрийг шалгахад зориулан өмнөх гэрчилгээнүүдийг агуулна.
- Нийтийн түлхүүрийн дэд бүтцэд ашиглагдах гэрчилгээнүүдийг
- Хүчингүй гэрчилгээнүүдийн жагсаалт
- Гэрчилгээний бодлогын одоо байгаа болон өмнөх хувилбарууд

- Албан ёсны холбоо барих хаяг (э-мэйл хаягийг оруулаад)
- Гэрчилгээ олгох байгууллагад холбоотой бусад үйлчилгээний тухай мэдээлэл

2.3 Хэвлэн нийтлэх цаг хугацааны давтамж

Гэрчилгээг үүссэн даруйд хэвлэн нийтэлнэ. Гэрчилгээ хүчингүй болсон эсвэл гэрчилгээний хугацаа дуусахаас 7 хоногийн өмнө хүчингүй гэрчилгээний жагсаалтыг шинэчилж 6 цагийн дотор хэвлэнэ. Гэрчилгээний бодлого болон гэрчилгээний үйл ажиллагааны журмын шинэ хувилбар батлагдах даруйд хэвлэн нийтэлнэ. Тусгай зөвшөөрөл эзэмшигч ГБ нь ГҮАЖ, “Гэрчилгээ эзэмших гэрээ” эсвэл “Хэрэглэгчийн үйлчилгээний нөхцөл”-д оруулсан өөрчлөлтийг баталгаажуулснаас хойш 7 хоногийн дотор нийтлэх үүрэгтэй.

2.4 Хадгалах байранд нэвтрэх

Гэрчилгээ олгох байгууллагын веб серверийн мэдээлэлд хандахад ямар ч хязгаарлалтгүй байх ба зөвхөн унших эрхтэйгээр нээлттэй байна. Хэрэв өгөгдлийг буруугаар ашиглаж байгаа нь тодорхой байвал эзэмшигчдийг гэрчилгээг хамгаалах зорилгоор хандалтын удирдлага идэвхжин хандалтад хязгаарлалт хийж болно. Веб серверийн техникийн үйлчилгээ долоо хоног бүр нэг цаг байх ба үйлчилгээний хуваарийг энэ веб дээр байршуулна. Веб сервер дээр техникийн үйлчилгээ хийж байх цаг хугацаанд бүх хандалтууд хаагдсан байна.

3. Таних ба баталгаажуулах

3.1 Нэршил

3.1.1 Нэршлийн төрлүүд

Гэрчилгээ авахыг хүсэгчийн нэршил нь X.509 стандартын дагуу доор дурдагдсан хэлбэртэй байна:

a) Хувь хүний гэрчилгээ нь тухайн хүний бүтэн нэрийг агуулсан байна.
b) Аж ахуйн нэгжийн гэрчилгээ нь тухайн оролцогч болон серверийг бүрэн илэрхийлэх шаардлага хангасан домайн нэр байна.

3.1.2 Нэршлийн утга

Нэршил нь тухайн захиалагчийг илэрхийлэх, хүнд энгийн байдлаар ойлгогдох хэлбэртэй байх ба захиалагчийг баталгаажуулах нэртэй заавал тодорхой үндэслэлтэйгээр холбогдсон байхаар үүсгэнэ.

3.1.3 Нэргүй эсвэл нууц нэр ашигласан захиалагчид

Гэрчилгээ олгох байгууллага нь нэргүй эсвэл нууц нэр ашигласан захиалагчид гарын үсэг зурахгүй.

3.1.4 Төрөл бүрийн нэрний хэлбэрийг хөрвүүлэх дүрмүүд

a) Хуулийн этгээд бүр тодорхой ба дахин давтагдашгүй нэрийг гэрчилгээний агуулгын талбарт ашиглана.
b) Энэхүү баримт бичигт агуулагдаж буй аливаа нэр нь “C=MN, O=CA” үүнийг агуулна. Захиалагчдыг “Хүмүүс” эсвэл “Оролцогч” гэсэн ангилалд хуваах бөгөөд “O=Гэрчилгээний баг” маягтад тусгагдсан байна. “Хүмүүс” гэдэг ангилалд гэрчилгээ захиалагч бодит хүнийг оруулна. “Оролцогч” гэдэг ангилалд гэрчилгээ захиалагч аж ахуйн нэгжийн автомат систем эсвэл програм хангамжийг оруулна.
c) Хэрэглэгчийн гэрчилгээний хувьд ерөнхий нэр нь захиалагчийн бүтэн нэрийг агуулсан байна.
d) Хэрэв захиалагч нь “Оролцогч” ангилалд хамаарах бол гэрчилгээний агуулгын талбарт заавал оролцогч болон серверийг бүрэн илэрхийлэх шаардлага хангасан домайн нэрийг ашиглана.

3.1.5 Нэрний давтагдашгүй байдал

Гэрчилгээ олгох байгууллагаас үүсгэж буй бүх гэрчилгээнд тусгагдсан нэр нь хоёрдмол утгагүй, дахин давтагдашгүй байна. Хэрэв нэр нь дахин давтагдашгүй биш бол тоо болон үсгийг нэмэн дахин давтагдашгүй болгоно. Гэрчилгээ нь дахин давтагдашгүй хувь хүн болон эх сурвалжид л олгогдоно. Хэрэглэгч гэрчилгээг бусадтай хуваан ашиглаж болохгүй.

3.1.6 Хүлээн зөвшөөрөх, баталгаажуулах болон үйлдвэрийн тэмдгийн үүрэг

Нөхцөл байхгүй

3.2 Эхний удаа жинхлэн баталгаажуулах

3.2.1 Хувийн түлхүүрийг эзэмших баталгаажуулалтын арга

Гэрчилгээ олгох байгууллага нь хувийн түлхүүрийн эзэмшилтийг түүний гэрчилгээнд гарын үсэг зурах хүсэлт (CSR) – ээр баталгаажуулна.

3.2.2 Байгууллагын таних ба баталгаажуулах

Гэрчилгээ олгох байгууллага эсвэл бүртгэлийн нэгж нь аливаа аж ахуйн нэгжийн Улсын бүртгэлийн газраас олгосон гэрчилгээ эсвэл ТҮЦ машины хуулийн этгээдийн лавлагааны баримтыг үндэслэн таньж баталгаажуулна.

3.2.3 Хувь хүнийг таних ба баталгаажуулах

Гэрчилгээ олгох байгууллага эсвэл бүртгэлийн нэгж нь хувь хүнийг түүний иргэний үнэмлэх болон түүнтэй адилтгах баримт бичгийг үндэслэн таньж баталгаажуулна. Гадаадын иргэнийг Монгол Улсад оршин суух үнэмлэхийг нь ашиглан нотолно.

3.2.4 Захиалагчийн шалгагдаагүй мэдээлэл
Тусгайлсан нөхцөл байхгүй бөгөөд Гэрчилгээний Тусгайлсан Нэрийг X.500 стандартууд болон ASN.1 синтаксын хүрээнд тайлбарлаж, ойлгоно.

3.2.5 Баталгаажуулах газар
3.2.2 ба 3.2.3 хэсгийг харна уу.

3.2.6 Харилцан ажиллах нөхцөлүүд
Нөхцөл байхгүй.

3.3 Түлхүүр шинэчлэх хүсэлтийг таних ба баталгаажуулах

3.3.1 Түлхүүр шинэчлэх загварыг таних ба баталгаажуулах
Гэрчилгээний хугацаа дуусгавар болсон эсвэл түлхүүрийг шинэчлэх үед дахин шинээр бүртгүүлэх шаардлагатай. Гэрчилгээ олгох байгууллага нь шинээр бүртгүүлэх шаардлагатай гэсэн санамжийг тухайн хэрэглэгчийн эзэмшиж буй гэрчилгээний хугацаа дуусгавар болохоос нэг сарын өмнө мэдэгдэх ёстой. Хэрэглэгчийн гэрчилгээг нэг жил тутамд шинэчлэх шаардлагатай. Гэрчилгээний хугацаа дуусгавар болсны дараа түлхүүрийг шинэчлэх боломжгүй бол дахин шинээр анхан шатны бүртгүүлэлтийг хийнэ.

3.3.2 Хүчингүй болсны дараа түлхүүрийг шинэчлэх үйлдлийн таних ба баталгаажуулах
Хэрэв гэрчилгээ хүчингүй болсон бол түлхүүрийг шинэчлэх боломжгүй бөгөөд дахин шинээр анхан шатны бүртгүүлэлтийг хийнэ.

3.4 Хүчингүй болгох хүсэлтийг таних ба баталгаажуулах
Хэрэглэгч ба байгууллагын гэрчилгээг хүчингүй болгох хүсэлтийг гэрчилгээний үйл ажиллагааны журмын дагуу тэдгээрийг баталгаажуулсан байгууллагын баримт бичгээр таньж баталгаажуулна. (3.2.2 ба 3.2.3 хэсгийг харна уу)

4. Гэрчилгээний амьдралын хугацааны үйл ажиллагааны шаардлага

4.1 Гэрчилгээний өргөдөл

4.1.1 Гэрчилгээний өргөдлийг хэн гаргаж болох вэ
Гэрчилгээний өргөдлийг гаргаж болох хүмүүсийг доор жагсаав
- Хувь хүн
- Хуулийн этгээд

4.1.2 Бүртгүүлэх үйл явдал ба түүний үүрэг
Хэрэглэгч “Гэрчилгээний байгууллагын бүртгүүлэх заавар”-т тусгагдсан үйлдлийн дагуу өөрийн компьютер дээр хувийн болон нийтийн түлхүүрийг үүсгэн тухайн нийтийн түлхүүрийг агуулж буй CSR хүсэлтийг бүртгэлийн нэгжид хүргэнэ. Хэрэв сүлжээ ашиглах бол тухайн дамжуулж буй шугам нь SSL нууцлалын протокол ашиглан шифрлэгдсэн байна. Нарийвчилсан зааврыг гэрчилгээний байгууллагын веб хуудас дээр байрлах “Гэрчилгээний байгууллагын бүртгүүлэх заавар”-т тусгасан.

4.2 Гэрчилгээний өргөдөлд ажиллах процесс

4.2.1 Таньж баталгаажуулах функцийг гүйцэтгэх
Хэрэглэгч гараар бөглөсөн өргөдлийн маягтыг Гэрчилгээний байгууллагын бүртгэлийн нэгжид бүртгүүлнэ.

4.2.2 Өргөдлийг баталгаажуулах эсвэл буцаах
Бүртгэлийн нэгж нь энэ баримт бичгийн 3.2.2 ба 3.2.6 хэсгийн шаардлагыг хангаж байгаа эсэхийг шалгана. Хэрэв 3.2 хэсгийн шаардлагыг хангахгүй бол өргөдлийг буцаах ба шаардлагыг хангавал Гэрчилгээний байгууллагад өргөдлийг баталгаажсан гэж мэдэгдэнэ. ГБ хуурамч баримтаар Гэрчилгээ авах өргөдөл гаргасан этгээдийг “Хар жагсаалт”-д бүртгэж, Гэрчилгээ авах өргөдлөөс татгалзах эрхтэй.

4.2.3 Гэрчилгээний өргөдөлд хариу өгөх хугацаа
Хүсэлтийг шалган баталгаажуулж дууссан даруйд гэрчилгээг үүсгэнэ. Ердийн үед энэхүү хугацаа нь ажлын 5 өдрөөс ихгүй байна.

4.3 Гэрчилгээг олгох

4.3.1 Гэрчилгээг олгоход Гэрчилгээний байгууллагын хийх үйлдэл
CSR –г Гэрчилгээний байгууллагын хувийн түлхүүрийг агуулсан, ямар нэг сүлжээнд холбогдоогүй компьютерт суулгана. Энэ компьютер дээр гэрчилгээг үүсгэн гарын үсэг зурна. Гарын үсэг зурагдсан гэрчилгээг буцаан Гэрчилгээний байгууллагын онлайн серверт байршуулна.

4.3.2 Гэрчилгээ үүсгэсэн тухай захиалагчид мэдэгдэх
Гэрчилгээ хүсэгчид түүний гэрчилгээг Гэрчилгээжүүлэх байгууллагын хувийн түлхүүрээр баталгаажуулсан эмайлээр илгээх ба мөн бүртгэлийн нэгжид мэдэгдэнэ.

4.4 Гэрчилгээ хүлээн зөвшөөрөх

4.4.1 Гэрчилгээг хүлээн зөвшөөрснийг тогтоох

Гэрчилгээ агуулсан эмайл хүлээн авсан захиалагч эмайлийн гарын үсгийг шалгана. Дараа нь хүлээн авсан гэрчилгээн доторх нийтийн түлхүүрийг өөрийн нийтийн түлхүүртэй тулган ямар нэг файлыг нийтийн түлхүүрээрээ шифрлэн түүнийг хувийн түлхүүрээрээ буцаан задлах үйлдлийг хийн шалгана. Гэрчилгээ хүсэгч тал өөрийн эзэмших гэрчилгээг шалгасны дараа Гэрчилгээний байгууллагад мэдэгдэнэ. Хэрэв шалгалт амжилттай болж ямар нэг асуудал гарахгүй бол хүсэгч тал Гэрчилгээний байгууллага болон харгалзах бүртгэлийн нэгжид заавал мэдэгдэнэ. Амжилтгүй болсон тохиолдолд хүсэгч тал Гэрчилгээний байгууллага болон харгалзах бүртгэлийн нэгжид гэрчилгээг хүлээн авахаас татгалзсан хариуг татгалзах болсон шалтгааны хамт заавал мэдэгдэнэ. Гэрчилгээг хүлээн зөвшөөрсөн талаар ямар нэг мэдээлэл нэг хүсэгчээс нэг сарын дотор ирэхгүй бол Гэрчилгээний байгууллага тухайн гэрчилгээг хүчингүй болгоно.

4.4.2 Гэрчилгээний байгууллага гэрчилгээг хэвлэн нийтлэх

Гэрчилгээний байгууллага гэрчилгээг хүлээн зөвшөөрсөн хариуг хүлээн аваад хадгалах байранд байршуулна (2.1 харна уу).

4.4.3 Гэрчилгээний байгууллагаас гэрчилгээ олгосон тухай бусад байгууллагуудад мэдэгдэх

Гэрчилгээний байгууллага нь гэрчилгээ олгосон тухай ямар нэг өөр байгууллагуудад мэдэгдэхгүй.

4.5 Түлхүүрийн хослол болон гэрчилгээний хэрэглээ

4.5.1 Захиалагчийн хувийн түлхүүр ба гэрчилгээний хэрэглээ

Гэрчилгээний байгууллагаас олгосон гэрчилгээ ба түүнд харгалзах хувийн түлхүүрүүд нь зөвхөн 1.4.1-д заасан зөвшөөрлийн дагуу ашиглагдана. Гэрчилгээг зөвхөн гэрчилгээн доторх зориулалт гэсэн талбарт заасан төрөлд ашиглана. Гэрчилгээ хүчингүй болох эсвэл хугацаа дуусах үед харгалзах хувийн түлхүүрүүд дахин ашиглах боломжгүй болно. Гэрчилгээ эзэмшигч нь гэрчилгээг зөвхөн ГБ –ийн Харилцаа холбооны тухай хуулийн 13.2.1, эсвэл ГҮАЖ –д заасан зорилгоор ашиглана. Гэрчилгээний хэрэглээ нь гэрчилгээний “*Key Usage”* талбарын утгатай нийцэлтэй байна. Гэрчилгээ эзэмшигч нь өөрийн хувийн түлхүүрийн нууцлал, аюулгүй байдлыг хариуцах ба гэрчилгээ хүчингүй болсон эсвэл цуцлагдсанаас хойш тухайн гэрчилгээнд хамаарах хувийн түлхүүрийг ашиглахгүй байх үүрэгтэй.

4.5.2 Хамаарах талын нийтийн түлхүүр болон гэрчилгээний хэрэглээ

Хамаарах тал нь гэрчилгээг үүсгэсэн Гэрчилгээний байгууллагыг шалгах талыг төлөөлнө

а) Энэ нь доорх нөхцөлд хүчин төгөлдөр байна

- Гэрчилгээний байгууллагаас олгогдсон гэрчилгээ мөн эсэхэд итгэхэд
- Гэрчилгээний хугацаа хүчинтэй эсэх
- Тухайн гэрчилгээг ашиглах үед Гэрчилгээний байгууллагын хүчингүй гэрчилгээний жагсаалттай тулгахад.

b) Гэрчилгээний бодлогын баримт бичигт тусгагдсаны дагуу түлхүүр болон гэрчилгээг ашиглаж буй эсэх.

4.6 Гэрчилгээг шинэчлэх

4.6.1 Гэрчилгээг шинэчлэх нөхцөл
Гэрчилгээний байгууллага нь хэрэглэгчийн гэрчилгээг шинэчлэхгүй. Захиалагч нь 4.7 хэсэгт заасны дагуу түлхүүрийг шинэчлэх ёстой.

4.6.2 Гэрчилгээг шинэчлэх хүсэлтийг хэн гаргах боломжтой вэ
4.6.1 хэсгийг харна уу.

4.6.3 Гэрчилгээг шинэчлэх хүсэлтийн процесс
4.6.1 хэсгийг харна уу.

4.6.4 Шинэ гэрчилгээ үүссэн талаар захиалагчид мэдэгдэх
4.6.1 хэсгийг харна уу.

4.6.5 Шинэчлэгдсэн гэрчилгээг хүлээн зөвшөөрөх удирдлага
4.6.1 хэсгийг харна уу.

4.6.6 Гэрчилгээний байгууллага шинэчлэгдсэн гэрчилгээг хэвлэн нийтлэх
4.6.1 хэсгийг харна уу.

4.6.7 Гэрчилгээний байгууллага шинэчлэгдсэн гэрчилгээг бусад байгууллагуудад мэдэгдэх
4.6.1 хэсгийг харна уу.

4.7 Гэрчилгээний түлхүүрийг шинэчлэх

4.7.1 Түлхүүрийг шинэчлэх нөхцөл
Гэрчилгээ эзэмшигч нь дараах нөхцөлүүдэд түлхүүрийн хосыг дахин үүсгэх ёстой:

a) Гэрчилгээний хугацаа дуусах;
b) Гэрчилгээг өөрчлөх/солих;
c) Хувийн түлхүүр алдагдсан;
d) Гэрчилгээнд тусгагдсан параметрүүд өөрчлөгдөх;

4.7.2 Хэн шинэ гэрчилгээ хүсэх боломжтой вэ
Хүчинтэй гэрчилгээ эзэмшигч шинээр гэрчилгээ хүсэх боломжтой.

4.7.3 Шинэ түлхүүр үүсгэхийг хүсэх процесс
Бүртгэлийн нэгжээс баталгаажсан хүсэлтийг хүлээн авснаар Гэрчилгээний байгууллага гэрчилгээг шинэчлэх процессыг эхлүүлнэ.

4.7.4 Захиалагчид шинэ гэрчилгээ үүсгэсэн тухай мэдэгдэх
4.3.2 хэсэгтэй адил байна.

4.7.5 Шинэчлэгдсэн түлхүүртэй гэрчилгээг хүлээн зөвшөөрөх
4.4.1 хэсэгтэй адил байна.

4.7.6 Гэрчилгээний байгууллагаас шинэчлэгдсэн түлхүүртэй гэрчилгээг хэвлэн нийтлэх
4.4.2 хэсэгтэй адил байна.

4.7.7 Гэрчилгээний байгууллагаас шинэчлэгдсэн түлхүүртэй гэрчилгээг бусад байгууллагуудад мэдэгдэх
4.4.3 хэсэгтэй ижил байна

4.8 Гэрчилгээний өөрчлөлт

4.8.1 Гэрчилгээг өөрчлөх нөхцөл
Гэрчилгээнүүд өөрчлөгдөх ёсгүй. Гэрчилгээг өөрчлөх тохиолдолд хуучин гэрчилгээг хүчингүй болгон шинээр түлхүүрийн хосыг бий болгож тухайн шинэ түлхүүртэй хамт өөрчлөгдөх мэдээллийг оруулан гэрчилгээг үүсгэнэ.

4.8.2 Гэрчилгээг өөрчлөх хүсэлтийг хэн гаргаж болох
Хэрэглэх боломжгүй.

4.8.3 Гэрчилгээг өөрчлөх хүсэлтийн процесс
Хэрэглэх боломжгүй.

4.8.4 Захиалагчид шинэ гэрчилгээ үүссэн тухай мэдэгдэх
Хэрэглэх боломжгүй.

4.8.5 Өөрчлөгдсөн гэрчилгээг хүлээн зөвшөөрөх удирдлага
Хэрэглэх боломжгүй.

4.8.6 Гэрчилгээний байгууллагаас өөрчлөлт орсон гэрчилгээг хэвлэн нийтлэх
Хэрэглэх боломжгүй.

4.8.7 Гэрчилгээний байгууллагаас өөрчлөлт орсон гэрчилгээг бусад байгууллагуудад мэдээлэх
Хэрэглэх боломжгүй.

4.9 Гэрчилгээг хүчингүй болгох, түдгэлзүүлэх

4.9.1 Хүчингүй болгох нөхцөл
Доорх нөхцөлүүдэд гэрчилгээг хүчингүй болгох ёстой:

a) гэрчилгээний хугацаа дуусгавар болсон;
b) хувийн түлхүүр задарсан, задрах боломж бүрдсэн тухай тоон гарын үсэг эзэмшигч тусгай зөвшөөрөл эзэмшигчид мэдэгдсэн;
c) гэрчилгээ эзэмшигч гэрчилгээгээ хүчингүй болгуулахаар бичгээр хүсэлт гаргасан;
d) гэрчилгээ эзэмшигч иргэн нас барсан, хуулийн этгээд татан буугдсан;
e) гэрчилгээг авахдаа хуурамч баримт бичиг бүрдүүлсэн нь тогтоогдсон;
f) гэрчилгээ эзэмшигч Цахим гарын үсгийн тухай хуулийн 16.2-т заасан үүргээ биелүүлээгүй.

Гэрчилгээний байгууллагын хувийн түлхүүр задарсан эсвэл гэрчилгээний байгууллагын хувийн түлхүүрээр баталгаажсан бүх гэрчилгээнүүд алдагдсан бол бүх гэрчилгээг хүчингүй болгоно.

4.9.2 Хүчингүй болгох хүсэлтийг хэн гаргах вэ
Гэрчилгээг хүчингүй болгох хүсэлтийг доорх этгээдүүд гаргана.

a) Гэрчилгээ эзэмшигч
b) Гэрчилгээний байгууллага болон бүртгэлийн нэгж мэдээллээ алдсан болон задарсан нь батлагдвал
c) Гэрчилгээнд агуулагдаж буй агуулгыг хүчингүй болгохыг тухайн байгууллага хүсвэл

4.9.3 Хүчингүй болгох хүсэлтийн процесс
Өөрчлөлтийн хүсэлтийг зөвхөн баталгаажсан гэрчилгээг эзэмшигч онлайн хэрэгсэл ашиглан гаргана. Ослын тохиолдолд гэрчилгээ эзэмшигч өөрийн биеэр яаралтай бүртгэлийн нэгжид ирж хүчингүй болгох хүсэлтийг гаргана. Гэрчилгээг хүчингүй болгохын өмнө Гэрчилгээний байгууллага хүсэлт гаргасан этгээдийг тоон гарын үсгийг шалгаж баталгаажуулна.

4.9.4 Хүчингүй болгох хүсэлтийг гаргах эрх зүйн хугацаа
Хүчингүй болгох хүсэлтийг гаргах эрх зүйн хугацаа гэж байхгүй. Баталгаажсан хүсэлтийг хүлээн авсан даруйд Гэрчилгээний байгууллага боломжит хамгийн хурднаар хүчингүй болсон тухай мэдээллийг хэвлэн

нийтлэнэ.Харин хүчингүй болгосон эсвэл түдгэлзүүлсэн тохиолдолд 6 цагийн дотор хэвлэн нийтэлнэ.

4.9.5 Хүчингүй болгох хүсэлтэд хариу үйлдэл хийх хугацаа
Гэрчилгээний байгууллага нь энгийн үед ажлын 1 өдрийн дотор гэрчилгээг хүчингүй болгох үйл ажиллагааг явуулна.

4.9.6 Хамаарагч талуудад зориулсан хүчингүй болсныг шалгах шаардлага
Гэрчилгээг ашиглахын өмнө хамаарагч тал нь Гэрчилгээний байгууллагын хэвлэн нийтэлсэн хүчингүй гэрчилгээний жагсаалттай тухайн гэрчилгээг тулган хүчин төгөлдөр эсэхийг баталгаажуулна.

4.9.7 Хүчингүй гэрчилгээний жагсаалтыг шинэчлэх давтамж (боломжтой бол)
Гэрчилгээний байгууллага нь аливаа гэрчилгээ хүчингүй болсон болон гэрчилгээний хугацаа дуусахаас 7 хоногийн өмнө шинэчлэн хэвлэн нийтэлнэ.

4.9.8 Хүчингүй гэрчилгээний жагсаалтыг үүсгэх хугацааны хамгийн их хоцрогдол (боломжтой бол)
Аливаа сүлжээнд холбогдоогүй гэрчилгээний систем дээр үүсгэсэн хүчингүй гэрчилгээний жагсаалтыг тэр даруйд хугацааны сааталгүй зөөврийн төхөөрөмжөөр хуулан онлайн хадгалах байранд байршуулна.

4.9.9 Гэрчилгээг хүчингүй болгосон тухай мэдээллийг онлайнаар шалгах боломж
Хамгийн сүүлийн хүчингүй гэрчилгээний жагсаалт нь Гэрчилгээний байгууллагын веб хуудас дээр байна. Гэрчилгээний байгууллага нь хадгалах байрнаас хамаарч хүчингүй гэрчилгээний жагсаалтыг хэвлэн нийтэлнэ (2.1 харна уу). Өөр ямар нэгэн онлайн шалгах боломж байхгүй.

4.9.10 Хүчингүй гэрчилгээг онлайнаар шалгахад тавигдах шаардлага
Хамаарагч талууд гэрчилгээ ашиглах болон түүнд итгэхийн өмнө хүчингүй гэрчилгээний жагсаалтыг Гэрчилгээний байгууллагын веб хуудаснаас шалгах ёстой. Хүчингүй гэрчилгээний жагсаалтыг шалгахад ямар нэг хандалтын хязгаарлалт байхгүй.

4.9.11 Хүчингүй болсныг зарлах бусад төрлүүд
Одоогоор хүчингүй болсныг зарлах өөр төрөл байхгүй.

4.9.12 Түлхүүр алдагдах тухай тусгай шаардлага
ГБ нь өөрийн хувийн түлхүүрийг задарсан гэж үзвэл нэн даруй хэрэглэгчдэд мэдэгдэх үүрэгтэй ба тусгайлсан нөхцөл байхгүй.

4.9.13 Түдгэлзүүлэх нөхцөл

Цахим гарын үсгийн тухай хуулийн 13.1 –р зүйлд заасан нөхцөл үүсвэл түдгэлзүүлнэ.

4.9.14 Хэн түдгэлзүүлэх хүсэлт гаргах вэ

Гэрчилгээ эзэмшигч түдгэлзүүлэх хүсэлт гаргах эрхтэй.

4.9.15 Түдгэлзүүлэх хүсэлтийн процесс

Түдгэлзүүлэх хүсэлтийг хүлээн авч тухай гэрчилгээг түр CRL оруулан хэвлэн нийтэлнэ.

4.9.16 Түдгэлзүүлэх хугацааны хязгаарлалт

Гэрчилгээ эзэмшигчийн хүсэлтээр эсвэл тухайн гэрчилгээний хугацаа дуусах хүртэл

4.10 Гэрчилгээний төлөв байдлын үйлчилгээ

4.10.1 Үйл ажиллагааны шинж чанар

Гэрчилгээний байгууллага нь доорх мэдээллүүдийг өөрийн хадгалах байранд байршуулан веб хуудсаараа дамжуулан тэдгээрт хандах боломжийг бий болгоно. (LDAP and OCSP)

- Гэрчилгээний байгууллагыг илэрхийлэх үндсэн гэрчилгээ
- Бүх олгосон хүчинтэй гэрчилгээнүүд
- Хүчингүй гэрчилгээний жагсаалт (сүүлчийн байдлаар)

4.10.2 Үйлчилгээний бэлэн байдал

Онлайн хадгалах байранд тогтмол үр дүнтэй үйлчилгээг хийх ба 24х7 цагаар хандах боломжтой байна.

4.10.3 Бусад боломжууд

Нөхцөл байхгүй.

4.11 Тоон гарын үсэг дуусгах

Хэрэв гэрчилгээний хугацаа дуусахаас өмнө сунгагдаагүй бол тухайн гарын үсэг гэрчилгээний хугацаа дууссанаар дуусгавар болно. Захиалагч гэрчилгээний хугацаа дуусахаас өмнө гэрчилгээг хүчингүй болгох хүсэлт гаргавал гарын үсэг гэрчилгээний хугацаа дуусахаас өмнө дуусгавар болно.

4.12 Түлхүүрийг хадгалалт ба сэргээх

4.12.1 Түлхүүрийг хадгалах ба сэргээх бодлого болон журам

Түлхүүрийг хадгалах ба сэргээх үйлчилгээ үзүүлэхгүй. Түлхүүр эзэмшигч нь түлхүүрийг алдахаас хамгаалах бүх аргыг өөрөө хариуцна.

4.12.2 Холболтын түлхүүрийг багцлах болон сэргээх бодлого ба журам
4.12.1 хэсгийг харна уу.

5. Тоног төхөөрөмж, удирдлага, үйл ажиллагааны хяналт

5.1 Физик удирдлага

5.1.1 Барилгын байршил болон байгууламж
Гэрчилгээний байгууллага нь энэхүү баримт бичгийг удирддаг байгууллагын хаягийн байршилтай хамт байрлана. (1.5.2 хэс гийг харна уу).

5.1.2 Физик хандалт
Гэрчилгээний байгууллагын тоног төхөөрөмжийн орчин Үндэсний Дата Төвийн байранд байрлах ба нь зөвхөн тухайн орчинд хандах эрх хүмүүсийн хяналтад байна.

5.1.3 Хүчдэл ба агааржуулалт
Офлайн болон онлайн холболттой Гэрчилгээний байгууллагын серверүүд байрлах өрөө нь агааржуулагчтай байна. Серверүүд нөөц тэжээлд залгагдсан байх ба энэхүү нөөц тэжээл нь цахилгаан тасарсан үед 1 цагийн турш цахилгаанаар хангах боломжтой байна.

5.1.4 Усны хамгаалалт
5.1.2 харах

5.1.5 Галын дохиолол, хамгаалалт
Монгол улсын хуульд заасны дагуу серверийн өрөөнд галын дохиоллын системийг суурилуулна.

5.1.6 Мэдээлэл хадгалагч
Зөөврийн мэдээлэл хадгалагчид мэдээллийг хуулбарлан зөвхөн эрх бүхий хүн хандах эрхтэй цоожтой сейфэнд хадгална.

5.1.7 Хаягдлыг зайлуулах
Хаягдал өгөгдөл (криптографтай холбогдолтой өгөгдөл жишээ нь хувийн түлхүүр, нэвтрэх хэллэг, хувийн мэдээлэл) нь хамгаалагдсан байх ба мэдээллийг дахин ашиглахгүй гэсэн баталгаагаар ханган хамгаалагдсан хаягдал өгөгдлийг цэвэрлэнэ.

5.1.8 Алсаас нөөцлөх
Алсаас нөөцлөх үйлдлийг одоогийн байдлаар гүйцэтгэхгүй.

5.2 Процедурын удирдлага

5.2.1 Итгэлцлийн талууд
Найдвартай дэд бүтцийг зохицуулах ажлыг гүйцэтгэх ажилтнууд, гэрээгээр ажиллагчид, зөвлөхүүдийг итгэлтэй хүмүүс гэж үзнэ.

5.2.2 Даалгавар тус бүрт шаардагдах хүмүүсийн тоо
Шаардлагатай тооны хүмүүсийг ажиллуулах ба хамгийн багадаа 2 жил хамтран ажиллах нөхцөлтэй байна.

5.2.3 Тал бүрийг таних ба баталгаажуулах
ГБ өөрийн журмын дагуу баталгаажуулан өөрсдөө тогтооно.

5.2.4 Давхар үүргийг салгах шаардлагатай талууд
Нэг ажилтан 2 үүргийг давхар гүйцэтгэхгүй.

5.3 Боловсон хүчний удирдлага

5.3.1 Мэргэшил, туршлага ба чанарын шаардлагууд
Гэрчилгээний байгууллагын бүх ажилтнууд системийг удирдах болон анализ хийх туршлагатай байна.

5.3.2 Далд шалгах үйл ажиллагаа
Нөхцөл байхгүй

5.3.3 Сургалтын шаардлагууд
Гэрчилгээний байгууллага болон бүртгэлийн нэгжийн операторуудад дотоод сургалтыг явуулна.

5.3.4 Дахин сургах хугацаа, шаардлагууд
Байгууллагын үйл ажиллагаа шинэчлэгдэх, шинэ програм хангамж сууриулуулагдах болон програмд нэмэлт өөрчлөлт хийх бүрт сургалтыг зохион байгуулна.

5.3.5 Ажлын дарааллын давтамж, эрэмбэ
Нөхцөл байхгүй

5.3.6 Зөвшөөрөгдөөгүй үйлдлүүдийн хориг арга хэмжээ
Гэрчилгээний байгууллага нь зөвшөөрөгдөөгүй үйлдлүүдэд Монгол улсын хуулийн заалтын дагуу хуулийн хариуцлага хүлээлгэх эрхтэй.

5.3.7 Бие даасан гэрээний ажилтны шаардлагууд
Нөхцөл байхгүй

5.3.8 Ажилтнуудыг баримтжуулалтаар хангах
Бүх Гэрчилгээний байгууллагын ажилтнууд даалгавраа амжилттай гүйцэтгэхэд шаардагдах бүх баримт бичгээр хангагдсан байх ёстой.

5.4 Хяналтын бүртгэлийн процедурууд

5.4.1 Бичигдсэн үйлдлийн төрлүүд
Дараах үйлдлүүд бичигдсэн байна.

a) Гэрчилгээний байгууллагын хост

- нэвтрэх/гарах/дахин ачаалах
- гэрчилгээнүүдийг үүсгэх, гэрчилгээнүүдийг хүчингүй болгох
- систем ачаалах болон унтраах

b) Гэрчилгээний байгууллагын веб онлайн сервер

- гэрчилгээний хүсэлтийн хүлээн авалт
- гэрчилгээнүүдийг бий болгох
- гэрчилгээний хүчингүй болгох хүсэлтийг хүлээн авалт
- бүртгэлийн нэгжийн гэрчилгээний хүсэлтийн баталгаажуулалт
- гэрчилгээний хүчингүй болголт
- Хүчингүй гэрчилгээний жагсаалтыг бий болгох

5.4.2 Үйл ажиллагааны бүртгэлийн давтамж

Бүртгэлийн файлуудыг сард нэг удаа шинжлэх, эсвэл мэдэгдэж байгаа болон сэжиглэгдэж байгаа хамгаалалтын цоорхой байх үед уг ажлыг хийнэ.

5.4.3 Хяналтын бүртгэлийг хадгалах хугацаа

Хяналтын бүртгэлийг хадгалах хугацаа хамгийн багадаа 10жил байна.

5.4.4 Хяналтын бүртгэлийн хамгаалалт

Хяналтын бүртгэлд зөвхөн Гэрчилгээний байгууллагын оператор, менежерүүд хандана.

5.4.5 Хяналтын бүртгэлийг нөөцлөх процедурууд

Амралтын болон баярын өдрүүдээс бусад өдрүүдэд орой бүр зөөврийн дискэнд архивын бүртгэлийг нөөцлөн авна.

5.4.6 Хяналтын цуглуулгын систем

Хяналтын бүртгэлийг цуглуулах систем бол Гэрчилгээний байгууллагын дотоод систем юм.

5.4.7 Субъектийн үйлдлийн шалтгааныг тэмдэглэх

ГБ өөрөө тогтооно

5.4.8 Эмзэг байдлын үнэлгээ

ГБ тогтмол эмзэг байдлыг үнэлгээг хийнэ.

5.5 Бичлэгүүдийн архив

5.5.1 Архивлагдсан бичлэгүүдийн төрөл

5.4.1 хэсгийг харна уу.

5.5.2 Архивын хадгалах хугацаа

Хамгийн бага хадгалах хугацаа 10 жил

5.5.3 Архивын хамгаалалт

Архив руу зөвхөн Гэрчилгээний байгууллагын оператор болон удирдлагын хүн хандана.

5.5.4 Архивлах, нөөцлөх үйл явц

Бичлэгүүд зөөврийн хэрэгсэл дээр нөөцлөгдөн хязгаарлагдмал хандалттай өрөөнд хадгалагдана.

5.5.5 Бичлэгүүдийг цаг хугацааг тэмдэглэх шаардлага.

Бүх үйл явдлын бичлэгүүдийн цаг хугацаа тэмдэглэгдсэн байна.

5.5.6 Архивын цуглуулгын систем (гадаад болон дотоод)

Гэрчилгээний байгууллагын архивын цуглуулгын систем нь дотоод үйл ажиллагаа байна.

5.5.7 Архивын мэдээллийг тогтоох болон хангах процедурууд

ГБ өөрөө тогтооно.

5.6 Түлхүүр шилжүүлэлт

Хэрэглэгчдийн түлхүүрийн хүчинтэй байдлыг тасалдуулахаас зайлсхийн хуучин Гэрчилгээний байгууллагын түлхүүрийн хугацаа дуусахаас нэг жилийн өмнө шинэ хувийн түлхүүрийг үүсгэнэ. Шинэ нийтийн түлхүүрийг онлайн хадгалах байранд байршуулах ба шинэ гэрчилгээнүүдийг үүсгэж болно.

5.7 Задрах үйл ажиллагаа болон яаралтай сэргээх

5.7.1 Будлиан болон задрах үйл ажиллагааны үед ажиллах

a) Хэрэглэгчийн түлхүүр алдагдсан эсвэл түүний компьютерийн гэмтлээс алдагдсан тохиолдолд харъяалах бүртгэлийн нэгжид нь нэн даруй мэдэгдэн гэрчилгээг сэргээх процессийг эхлүүлнэ.

b) Хэрвээ бүртгэлийн нэгжийн операторын хувийн түлхүүр задарсан эсвэл задарсан гэж сэжиглэж байвал бүртгэлийн нэгжийн оператор эсвэл менежер Гэрчилгээний байгууллагад заавал мэдэгдэж бүртгэлийн нэгжийн операторын гэрчилгээг сэргээх хүсэлтийг тавина.

c) Хэрэв тоон гарын үсгийн гэрчилгээ олгох байгууллагын хувийн түлхүүр задарсан эсвэл задарсан гэж сэжиглэж байвал доорх үйлдлүүдийг хийнэ.

- Бүртгэлийн нэгжүүд, захиалагчид, харилцагч талууд, харилцан баталгаажуулалт хийдэг тоон гарын үсгийн гэрчилгээ олгогч байгууллагуудад мэдэгдэнэ.
- Задарсан түлхүүрээр баталгаажсан гэрчилгээнүүд болон хүчингүй гэрчилгээний жагсаалтыг бий болгохыг зогсооно.

5.7.2 Тооцоолох нөөц, програм хангамж, ба/ эсвэл өгөгдөл эвдэрсэн.

Гэрчилгээний байгууллага хамгийн үр дүнтэй байдлаар сэргээх үйл ажиллагааг явуулна. Гэрчилгээний байгууллага сүйдсэн тохиолдолд маш яаралтай авч болох арга хэмжээнүүд авахын тулд доорх үйлдлүүдийг хийж гүйцэтгэнэ.

- Гэрчилгээний байгууллагын бүх тоон гарын үсгийн програм хангамжийн шинэ хувилбар болон ямар нэгэн шинэ бүрдэл хэсэг суурилуулагдах бүрт зөөврийн төхөөрөмж рүү тэдгээрийг

нөөцлөн авна.

- Гэрчилгээний байгууллага дээр хадгалагдаж буй өгөгдөлд өөрчлөлт орох бүрт зөөврийн төхөөрөмж рүү тэдгээрийг нөөцлөн авна.

Хэрэв системийн үйл ажиллагаа доголдвол тухайн тоног төхөөрөмж болон програм хангамжийн хамгийн сүүлийн тогтвортой байсан төлөвийг зөвхөн унших боломжтой нөөцийн хэсгээс ачаалан ажиллуулна. Хэрэв Гэрчилгээний байгууллагын хувийн түлхүүрийн бүх шифрлэгдсэн хуулбар устаагүй, алдагдаагүй болон задраагүй бол бүх гэрчилгээг хүчингүй болголгүйгээр үйл ажиллагааг даруй эхлүүлнэ.

5.7.3 Хэрэглэгчийн хувийн түлхүүр алдагдах үйл ажиллагаа

Хэрэглэгч болон бүртгэлийн хэсгийн түлхүүр задарсан тохиолдолд тухайн түлхүүрт харгалзах гэрчилгээг хүчингүй болгоно. Бүх харилцагч талууд үүнийг мэдвэл түлхүүрийн эзэмшигчид мэдэгдэх хэрэгтэй.

Гэрчилгээний байгууллагын хувийн түлхүүр задарсан тохиолдолд доорх үйлдлүүдийг хийнэ.

- Хамаарах бүх захиалагч болон бүртгэлийн нэгжүүдэд мэдэгдэнэ.
- Хүчингүй гэрчилгээний жагсаалтууд болон гэрчилгээг үүсгэх үйл ажиллагааг зогсооно.
- Задарсан гэрчилгээг сэргээх хүсэлтийг гаргана.
- Гэрчилгээний байгууллагын хувийн түлхүүрийг шинээр бий болгож түүнийг хэвлэн нийтэлж хадгалах газар байршуулна.
- Задарсан түлхүүрээр гарын үсэг зурагдсан бүх гэрчилгээнүүдийг хүчингүй болгож шинээр хүчингүй гэрчилгээний жагсаалтыг үүсгэн хэвлэж хадгалах газар байршуулна.

5.7.4 Яаралтай тусламжийн дараах бизнесийн үйл ажиллагааны чадамж

Тухайн нөхцөл байдлыг үнэлсний дараа ГБ-ын удирдлага тогтооно.

5.8 Гэрчилгээний байгууллага эсвэл бүртгэлийн нэгжийн үйл ажиллагааг зогсоох

Гэрчилгээний байгууллагын үйл ажиллагааг зогсоохоос өмнө дараах үйчилгээнүүд хийгдэнэ.

- Гэрчилгээний байгууллагад хамаарах бүртгэлийн нэгжүүд болон харилцагчид мэдээлэх
- Үйл ажиллагаа зогсох болсон тухай мэдээллийг аль болох сайн өргөн түгээх
- Гэрчилгээ олголтыг зогсоох
- Бүх гэрчилгээнүүдийг хүчингүй болгох
- Хүчингүй гэрчилгээний жагсаалтыг хэвлэн нийтлэх
- Хувийн түлхүүр болон түүний бүх хуулбарыг устгах

6. Техникийн аюулгүй байдлын хяналт

6.1 Түлхүүрийн хосыг үүсгэх, суулгах

6.1.1 Түлхүүрийн хосыг үүсгэх

Гэрчилгээний байгууллагын эрх бүхий ажилтан нь тусгайлсан програм хангамжийг ашиглан, сүлжээнд холбогдоогүй компьютер дээр Гэрчилгээний байгууллагын түлхүүрүүдийг үүсгэнэ. Хувь хүнд зориулсан (бүртгэлийн нэгжийн төлөөлөгчийг оролцуулан), компьютер эсвэл үйлчилгээ үзүүлэх түлхүүрийг түүнийг эзэмших эрхтэй этгээдийн хүсэлтийг үндэслэн системд нь үүсгэнэ.

6.1.2 Хувийн түлхүүрийг захиалагчид хүргэх

Захиалагч бүр өөрийн түлхүүрүүдтэй байна. Гэрчилгээний байгууллага нь захиалагчийн хувийн түлхүүрийг үүсгэхгүй. Хэрэглэгчийн тоон гарын үсгээс өөр зорилгоор үүсгэх хувийн түлхүүрийн хувийг ГБ хэрэглэгчийн өмнөөс үүсгэсэн бол (жишээ нь SSL) түлхүүрийн хос болон гэрчилгээг PKCS#12 стандарт форматад оруулан илгээнэ. PKCS#12 файлыг 16 оронтой нууц үгээр хамгаалах бөгөөд уг нууц үгийг ГБ –ийн системээс санамсаргүй үүсгэсэн 8 оронтой тоо ба түүний араас хэрэглэгчийн сонгосон 8 оронтой тоог нийлүүлэн бүрдүүлнэ.

6.1.3 Нийтийн түлхүүрийг гэрчилгээ хүсэгчид хүргэх

ГБ–д эцсийн хэрэглэгч болон БН нь нийтийн түлхүүрийг PKCS#10 Гэрчилгээнд Гарын Үсэг Зурах Хүсэлт (CSR) эсвэл SSL холболт ашиглан тоон гарын үсгээр баталгаажсан багцаар илгээнэ.

6.1.4 Гэрчилгээ олгох байгууллагын нийтийн түлхүүрийг (хамааралтай этгээд) өгөх

Гэрчилгээний байгууллагын гэрчилгээг хадгалах байрнаас татаж авч болно. (2.1 заалтыг харна уу)

6.1.5 Түлхүүрийн хэмжээ

Хэрэглэгчийн түлхүүрийн хэмжээ 2048 битээс багагүй байна. Гэрчилгээ олгох байгууллагын түлхүүр 4096 битээс багагүй байна. Гарын үсгийн алгоритм SHA256-аас багагүй байна.

6.1.6 Нийтийн түлхүүрийн өгөгдөл үүсгэх болон чанарыг шалгах

Тодорхойлогдоогүй.

6.1.7 Түлхүүр ашиглах зорилго (X.509 v3 стандартын түлхүүр ашиглах талбар)

Түлхүүрийг дараах төрлүүдэд ашиглаж болно. Үүнд:

а/ Хэрэглэгчийн гэрчилгээг

- Баталгаажуулах
- Татгалзахгүй байх
- Мэдээлэл ба түлхүүрийг шифрлэх
- Мэдээллийн бүрэн байдал
- Холболт тогтооход
- Итгэмжлэлээр үүсгэх

б/ Гэрчилгээний байгууллагын гэрчилгээг

- Гэрчилгээг баталгаажуулах

- Хүчингүй гэрчилгээний жагсаалтыг баталгаажуулах

6.2 Хувийн түлхүүрийг хамгаалах ба криптографийн төхөөрөмжийн хяналт

6.2.1 Криптографийн төхөөрөмжийн стандарт ба хяналт
Гэрчилгээний байгууллагын хувийн түлхүүрийг FIPS140-2 level 3 стандартыг хангах криптографийн төхөөрөмжөөр хамгаалагдсан байх ба хамгаалалтын нууц үгийн 3 хүнд салган хадгална. Гэрчилгээний байгууллагын хувийн түлхүүрийг шифрлэн Гэрчилгээний байгууллагын сүлжээнд холбогдоогүй компьютерт хадгална.

6.2.2 Хувийн түлхүүрийн олон талын хяналт
Гэрчилгээний байгууллага болон түүний салбарууд нь хувийн түлхүүрт олон талын хяналтыг хэрэгжүүлэхгүй. Гэхдээ Гэрчилгээний байгууллага олон талт хяналтыг 5.1.2-т тодорхойлсноор байгууллагынхаа серверийн хандалтыг хянахад хэрэглэнэ. Гэрчилгээний байгууллагын хувийн түлхүүрийн нөөцийг хийж гүйцэтгэхэд олон талын хяналт дор гүйцэтгэнэ.

6.2.3 Хувийн түлхүүрийг гуравдагч этгээдэд хадгалах
Хувийн түлхүүрийг гуравдагч этгээдэд хадгалуулахгүй.

6.2.4 Хувийн түлхүүрийг нөөцлөх
Гэрчилгээний байгууллагын хувийн түлхүүр нь шифрлэгдсэн байдлаар зөөврийн хадгалах төхөөрөмжид нөөцлөгдөх бөгөөд уг төхөөрөмжийг байгууллагын серверийн өрөөнд хамгаалалттай сейфэнд байлгана.

6.2.5 Хувийн түлхүүрийн архив
Гэрчилгээний байгууллагын хувийн түлхүүр нь шифрлэгдсэн байдлаар зөөврийн хадгалах төхөөрөмжид нөөцлөгдөх бөгөөд уг төхөөрөмжийг байгууллагын серверийн өрөөнд хамгаалалттай сейфэнд байлгана.

6.2.6 Хувийн түлхүүрийг криптографийн төхөөрөмж рүү болон төхөөрөмжөөс татах
Нөхцөл байхгүй.

6.2.7 Хувийн түлхүүрийг криптографийн төхөөрөмжид хадгалах
Нөхцөл байхгүй.

6.2.8 Хувийн түлхүүрийг идэвхжүүлэх арга
Гэрчилгээний байгууллагын хувийн түлхүүрийг нууц үгийн тусламжтайгаар идэвхжүүлдэг байна.

6.2.9 Хувийн түлхүүрийн идэвхжлийг цуцлах арга
Текстен хэлбэрт байгаа уншиж болох хувийн түлхүүр нь зөвхөн шуурхай санах ойд хадгалагдах бөгөөд шаардлагатай үйл ажиллагаа дууссан үед санах ойгоос устгана.

6.2.10 Хувийн түлхүүрийг устгах арга
6.2.9-ийг харна уу.

6.2.11 Криптограф загварын зэрэглэл
FIPS 140-2 level 3.

6.3 Түлхүүрийг удирдах бусад хүчин зүйл

6.3.1 Нийтийн түлхүүрийн архив
Гэрчилгээний байгууллага нь олгосон бүх гэрчилгээг зөөврийн хадгалах төхөөрөмжид архивлаж сүлжээнд холбогдоогүй, хамгаалалттай өрөөнд хадгална.

6.3.2 Гэрчилгээний болон түлхүүрүүдийг ашиглах хугацаа
Хэрэглэгчид өөрсдөө түлхүүрүүдийн хосыг үүсгэх ба Гэрчилгээний байгууллага түүний хүчинтэй эсэх талаар тодорхойлж чадахгүй. Зөвхөн Гэрчилгээний байгууллагын гэрчилгээний бодлого, журамд заасны дагуу олгосон гэрчилгээний хүчинтэй эсэхийг тодорхойлно. Захиалагчид олгосон гэрчилгээний хүчинтэй хугацаа 1 жил байх бөгөөд Гэрчилгээний байгууллагын өөрийн гэрчилгээний хувьд хүчинтэй хугацаа 5 жил байна.

6.4 Өгөгдлийг идэвхжүүлэх

6.4.1 Өгөгдлийг идэвхжүүлэх, суулгах
Хувийн түлхүүр бүр 16-с дээш тэмдэгтээс бүрдсэн нууц үгээр хамгаалагдсан байх ба нууц үг нь ядаж нэг тоо ба нэг үсэг агуулсан, ядаж нэг жижиг үсэгтэй, нэг тэмдэгтийг олон давтаагүй, хэрэглэгчийн нэрийг агуулаагүй

6.4.2 Өгөгдөл идэвхжүүлэлтийг хамгаалах
Нууц үгийг зөвхөн шифрлэгдсэн хувийн түлхүүрийг эзэмшигч мэднэ. Хувийн түлхүүрийг хамгаалах нууц үгийг (машинаар унших боломжтой эсвэл цаасан дээр) нь хамгаалалттай газар хадгална.

6.4.3 Мэдээллийг идэвхжүүлэх бусад хүчин зүйл
Тодорхойлоогүй.

6.5 Компьютерийн аюулгүй байдлын хяналт

6.5.1 Тусгай компьютерийн аюулгүй байдлын техникийн шаардлага
Гэрчилгээний байгууллагын сервер дээр гэрчилгээний системээс өөр бусад үйлчилгээ, програм хангамжийг ачаалахгүй. Сервер дээр эрсдэлтэй нэмэлт пакет суулгах болон өөрчлөлт хийх бол Гэрчилгээний байгууллагын ажилтны шийдвэрээр хийж гүйцэтгэнэ.

6.5.2 Компьютерийн аюулгүй байдлын зэрэглэл
Аюулгүй байдлыг сайн хангасан байна.

6.6 Техникийн хяналтын мөчлөг

6.6.1 Системийн хяналт
ГБ тогтооно.

6.6.2 Аюулгүй байдлыг удирдах хяналт
ГБ тогтооно.

6.6.3 Аюулгүй байдлын хяналтын мөчлөг
ГБ тогтооно.

6.7 Сүлжээний аюулгүй байдлын хяналт
Гэрчилгээ олгох байгууллагын бүх компьютерүүд галт ханаар хамгаалагдсан байх ба шаардлагагүй бүх програм хангамжийн үйлчилгээг зогсоосон байна.

6.8 Цаг хугацааг тэмдэглэх
Гэрчилгээний байгууллагын онлайн серверүүд дээр үүсгэсэн бүх бичлэгүүдийн цаг нь албан ёсоор тодорхойлсон сүлжээний цагийг үндэслэн тэмдэглэгдсэн байна. Хүчингүй гэрчилгээний жагсаалтыг үүсгэж буй сүлжээнд холбогдоогүй системийн цагийг оператор гараараа тохируулна.

7. Гэрчилгээ, хүчингүй гэрчилгээний жагсаалт (CRL), OCSP шинж чанарууд

7.1 Гэрчилгээний шинж чанар
Гэрчилгээний байгууллагаас олгосон бүх гэрчилгээ RFC5280 стандартад заагдсан X.509 гэрчилгээний дагуу байна.

7.1.1 Хувилбарын дугаар
Гэрчилгээний байгууллага зөвхөн X.509 гэрчилгээний хувилбар3 дагуу гэрчилгээ олгоно.

7.1.2 Гэрчилгээний өргөтгөл
Гэрчилгээний байгууллагаас олгож буй X.509 v3 гэрчилгээний өргөтгөлүүд доорх хэлбэртэй байна:

Хувь хүний сертификатын хувьд:	
Үндсэн шаардлага	Critical, ca:false
Субьект түлхүүрийн нэр	Hash
Удирдлагын түлхүүрийн нэр	Keyid
Түлхүүрийн хэрэглээ	Critical, digitalSignature, nonRepudiation, KeyEncipherment, dataEncipherment
Өргөтгөсөн түлхүүрийн хэрэглээ	clientAuth, emailProtection, codeSigning, timeStamping
CRL тараах цэгүүд	URI
Сертификатын бодлогууд	OID

Сервер/үйлчилгээний сертификатын хувьд:	
Үндсэн шаардлага	Critical, ca:false
Субьект түлхүүрийн нэр	Hash
Удирдлагын түлхүүрийн нэр	Keyid
Түлхүүрийн хэрэглээ	Critical, digitalSignature, nonRepudiation, KeyEncipherment, dataEncipherment
Өргөтгөсөн түлхүүрийн хэрэглээ	clientAuth, emailProtection, codeSigning, timeStamping
CRL тараах цэгүүд	URI
Сертификатын бодлогууд	OID
Сертификат гаргагч байгууллагын сертификатын хувьд:	
Үндсэн шаардлага	Critical, ca:false
Субьект түлхүүрийн нэр	Hash
Удирдлагын түлхүүрийн нэр	Keyid
Түлхүүрийн хэрэглээ	Critical, digitalSignature, nonRepudiation, KeyEncipherment, dataEncipherment
Өргөтгөсөн түлхүүрийн хэрэглээ	clientAuth, emailProtection, codeSigning, timeStamping
CRL тараах цэгүүд	URI
Сертификатын бодлогууд	OID

7.1.3 Обьектыг таних алгоритмууд

Гэрчилгээний байгууллагаас олгосон гэрчилгээнд ашигладаг алгоритмын таних код нь доорх байдалтай байна:

a) Холимог функц: id-sha 1 1.3.14.3.2.26
b) Кодчлол: rsaEncryption 1.2.840.113549.1.1.1
c) Гарын үсэг: sha256WithRSAEncryption 1.2.840.113549.1.1.11

7.1.4 Нэрний хэлбэрүүд

Гэрчилгээний байгууллагаас олгосон бүх гэрчилгээнүүд тухайн нэгж бүр цорын ганц хоёрдмол утгагүй бусдаас ялгарах нэртэй байна. Ялгах нэр нь ITU-T Standards Recommendation X.501 тодорхойлсны дагуу бүтэцтэй байх бөгөөд X.501.

Гаргагч:
C=MN, O= Тридум Кей ГБ, CN=Сүлжээний баг
Субьект:
C=MN, O=Тридум Кей ГБ, OU=текст, CN=нэр овог
C=MN, O=Тридум Кей ГБ, OU=текст, CN=FQDN (Бүтэн домэйн нэр)

Субьектын зайнд дараахь шинж бүхий нэгжийн Ялгарах Нэр байна.

MN	Дээд төвшний домэйн (Монгол)
Тридум Кей ГБ	Гэрчилгээний байгууллагын домэйн
[]	[Байгууллагын]
Нэр [овог]	Ердийн нэр
[үйлчилгээ “/”] FQDN	

7.1.5 Нэрний хязгаарлалт

7.1.4, 3.1.2, 3.1.1 заалтуудад зааснаас өөр бусад нэрний хязгаарлалт байхгүй.

7.1.6 Гэрчилгээний бодлогын бичиг баримтыг тодорхойлох код

Гэрчилгээний байгууллагын бодлогын бичиг баримтын кодыг 1.2-т заасан.

7.1.7 Бодлогын хязгаарлалтын өгөгдлийн хэрэглээ

Нөхцөл байхгүй

7.1.8 Бодлого тодорхойлогчийн өгүүлбэр зүй, утга зүй

Нөхцөл байхгүй

7.1.9 Гэрчилгээний бодлогын өгөгдөлд зориулж утга зүйг боловсруулах

Нөхцөл байхгүй

7.2 Хүчингүй гэрчилгээний жагсаалтын шинж чанар

7.2.1 Хувилбарын дугаар

Гэрчилгээний байгууллага CRLv2 (RFC5280v2) стандартын дагуу хүчингүй гэрчилгээний жагсаалтыг үүсгэж, хэвлэн нийтэлнэ.

7.2.2 Хүчингүй гэрчилгээний жагсаалт болон түүнийг өргөтгөх

Гэрчилгээний байгууллага нь гэрчилгээг хүчингүй болгосон шалтгааныг харгалзалгүйгээр хүчингүй гэрчилгээний жагсаалтыг бий болгоно. Хүчингүй гэрчилгээний жагсаалтад гэрчилгээг хүчингүй болгосон шалтгааныг оруулахгүй.

Дараагийн хүчингүй гэрчилгээний жагсаалтыг бий болгох өдрийг тухайн хүчингүй гэрчилгээний жагсаалтад оруулна. Хүчингүй гэрчилгээ бий болбол тухайн заасан хугацаанаас өмнө хүчингүй гэрчилгээний жагсаалтыг гаргаж тавина.

Хүчингүй гэрчилгээний жагсаалтын өргөтгөлд дараах зүйлсийг оруулна:

- Түлхүүрийг таних баталгаажуулсан мэдээлэл
- Хүчингүй гэрчилгээний жагсаалтын дугаар

Хүчингүй гэрчилгээний жагсаалтын өргөтгөлд оруулж болох зүйлсийг оруулна:

- Хүчингүй гэрчилгээний жагсаалтын шалтгааны код
- Хүчингүй болох өдөр

7.3 OCSP (Онлайн гэрчилгээний төлөвийн протокол) шинж чанар

7.3.1 Хувилбарын дугаар

Нөхцөл байхгүй

7.3.2 OCSP өгөгдөл

Нөхцөл байхгүй

8. Биелүүлэлтийн хяналт шалгалт болон бусад үнэлгээ

8.1 Үнэлгээ давтамж болон нөхцөл байдал

Гэрчилгээний байгууллага жилд нэг удаа явуулж буй үйл ажиллагаа нь гэрчилгээний бодлого болон журамтай нийцэж байгаа эсэхэд дотоод хяналт шалгалтыг хийж гүйцэтгэнэ. Гэрчилгээний байгууллага жилд ядаж нэг удаа бүртгэлийн нэгжийн үйл ажиллагаа гэрчилгээний бодлого болон журамтай нийцэж байгаа эсэхийг шалгана.

8.2 Шалгагчийн чадамж

Гүйцэтгэлийн хяналт шалгалтын ажлыг хараат бус бие даасан гуравдагч этгээд буюу аудитын байгууллагаар гүйцэтгүүлнэ.

8.3 Шалгуулж буй нэгж болон шалгагчийн хоорондын хамаарал

Гүйцэтгэлийн хяналт шалгалтын ажлыг хараат бус бие даасан гуравдагч этгээд буюу аудитын байгууллагаар гүйцэтгүүлнэ. Энэхүү аудитын байгууллага нь ашиг сонирхлын зөрчилгүй байх ба тэдгээрийн үйл ажиллагаанд саад учруулахгүй байна.

8.4 Үнэлгээнд хамаарах сэдвүүд

Гэрчилгээний байгууллагын хамгийн сүүлд батлагдсан гэрчилгээний бодлого болон журамд заасан үйлчилгээнүүдийг хяналт шалгалтад хамруулна.

8.5 Үл нийцэх байдалд авах арга хэмжээ

Үнэлгээ шалгалтаар гэрчилгээний бодлого болон журмын баримт бичгийн заалт болон бодит байдал хоорондоо зөрчилдөж байгааг тогтоовол Гэрчилгээний байгууллага нэн даруй засах арга хэмжээ авна.

8.6 Үр дүнг танилцуулах

Шалгалтын үр дүнг шалгагч болон Гэрчилгээний байгууллага хоёр зөвшилцсөн протоколд тусгаж өгнө. Хэрэв талууд зөвшилцөлд хүрч чадахгүй бол тал тус бүр өөрийн хувилбараар тайланг боловсруулна. Үр дүнгийн талаарх талуудын тайланг аль алиныг нь танилцуулах ёстой.

9. Бусад бизнесийн болон хуулийн асуудлууд

9.1 Төлбөр

9.1.1 Гэрчилгээ үүсгэх эсвэл шинэчлэх төлбөрүүд
ГБ тогтооно.

9.1.2 Гэрчилгээ ашиглалтын төлбөр
ГБ тогтооно.

9.1.3 Хүчингүй болгох эсвэл төлөв байдлын мэдээлэлд хандах төлбөр
ГБ тогтооно.

9.1.4 Бусад үйлчилгээний төлбөр
ГБ тогтооно.

9.1.5 Төлбөрийг буцаан олгох бодлого
ГБ тогтооно.

9.2 Санхүүгийн хариуцлага

9.2.1 Даатгагдсан байдал
100 сая төгрөгийн хариуцлагын даатгал хийсэн байна.

9.2.2 Бусад хөрөнгө
ГБ тогтооно.

9.2.3 Хэрэглэгчийн баталгаа болон даатгалд хамрагдсан байдал
Хэрэглэгчийн даатгалыг ГБ хариуцахгүй.

9.3 Бизнесийн мэдээллийн нууцлал

9.3.1 Нууц мэдээллийн хүрээ
Нөхцөл байхгүй.

9.3.2 Нууц мэдээллийн хүрээнд багтахгүй мэдээлэл
Нөхцөл байхгүй.

9.3.3 Нууц мэдээллийг хамгаалах хариуцлага
Нөхцөл байхгүй.

9.4 Хувийн мэдээллийн нууцлал.

9.4.1 Хувийн мэдээллийн төлөвлөгөө.
Нөхцөл байхгүй.

9.4.2 Хувийн мэдээлэлд хамаарагдах зүйлс

Хэрвээ хэрэглэгч нь мэдээллээ олон нийтийнх гэж зарлаагүй нөхцөлд мэдээлэл нь нууцлалтай байх болно. Хэрэглэгчийн өгсөн түүнийг мөн гэх баримтууд нь мөн нууц байх ёстой.

9.4.3 Хувийн биш мэдээлэл

Шинээр гарсан гэрчилгээ болон хүчингүй гэрчилгээний жагсаалтад багтсан мэдээлэл нь нууц мэдээлэлд багтахгүй.

9.4.4 Хувийн мэдээллийг хамгаалах хариуцлага.

Хувийн мэдээлэлтэй танилцаж буй хүн болгон мэдээллийн аюулгүй байдлыг хангаж хуулийг даган мөрдөж бусдад ил тод болгохгүй байх ёстой.

9.4.5 Хувийн мэдээллийг ашиглах анхааруулга болон зөвшөөрөл.

Хэрэв Гэрчилгээний байгууллага болон түүний итгэмжлэгдсэн бүртгэлийн нэгж мэдээллийг хэрэглэхийг хүсвэл хэрэглэгчээс заавал бичгээр зөвшөөрөл хүсэх хэрэгтэй. Хэрэглэгч нь заавал зөвшөөрнө гэсэн ямар ч заалт байхгүй.

9.4.6 Мэдээллийг нээлттэй болгох шүүхийн болон удирдлагын дагаж мөрдөх явц.

Монголын хуулиар зөвхөн хуулийн захирамжаар хувийн мэдээллийг ил болгох боломжтой.

9.4.7 Бусад мэдээллийг ил тод болгох нөхцөл байдал.

Нөхцөл байхгүй.

9.5 Оюуны өмчийн эрх

Гэрчилгээний байгууллага шинээр үүсгэж буй гэрчилгээнд патентын эрх авах шаардлагагүй.

9.6 Төлөөлөл болон баталгаа

9.6.1 Гэрчилгээний байгууллагын төлөөлөл болон баталгаа

Гэрчилгээн дээр хэвлэгдсэн мэдээлэл болон хүчингүй гэрчилгээний жагсаалтыг Гэрчилгээний байгууллага өөрийн байгаа үнэн зөв мэдээллээр хийж гүйцэтгэнэ. Бусад төрлийн баталгааг гаргахгүй.

9.6.2 Бүртгэлийн нэгжийн төлөөлөл болон баталгаа

3.2.3 болон 3.2.2 д заагдсан талуудын хүсэлтээр бүх итгэмжлэгдсэн бүртгэлийн нэгжүүд нь хамгийн сайн мэдлэгээрээ таних үйл ажиллагааг явуулах болно. Бусад төрлийн баталгаа гаргахгүй.

9.6.3 Хэрэглэгчийн төлөөлөл болон баталгаа

Захиалагч нь гэрчилгээг ашиглах болон хамгаалах үүрэг хүлээх ба гэрчилгээний бодлого болон журамд заасны дагуу гэрчилгээнд заасан өдрөөс эхлэн гэрчилгээний түлхүүр нь хүчин төгөлдөр болно. Хэдий тийм ч захиалагч өөртөө хатуу дүрэм журмыг тогтоож болно.

Захиалагч заавал доорх зүйлсийг дагаж мөрдөнө:

- Энэ баримт бичигт тусгагдсан зүйлсийг уншин дагаж мөрдөх ёстой.

- Гэрчилгээг зөвхөн зөвшөөрөгдсөн зорилгоор ашиглана.
- Хувийн өгөгдлийг хадгалах болон ашиглахыг баталгаажуулах. (хуульд заасны дагуу)
- Зөвшөөрөлгүй хэрэглэгчид мэдээллээ илчлэх, гээгдэх зэргээс байнгын сэрэмжтэй байх эсвэл гэрчилгээтэй холбоотой хувийн түлхүүрийг ашиглахдаа доорх зүйлсийг анхаарах.Үүнд:
  - Хувийн түлхүүрт нэвтрэх нууц үгийг сайн сонгох ёстой.
  - Хувийн түлхүүрт нэвтрэх нууц үгийг бусдаас хамгаалах ёстой.
  - Хэрэв хувийн түлхүүр алдагдсан болон ил тод болсон тохиолдолд Гэрчилгээний байгууллага болон харилцагч талуудад мэдэгдэх ёстой.
  - Гэрчилгээг ашиглахаа больсон болон гэрчилгээнд тусгагдсан мэдээллийг өөрчлүүлэх бол хүчингүй болгох хүсэлт гаргах ёстой. Мөн гэрчилгээний бодлого болон журамд заагдсан нөхцөлийг зөрчсөн тохиолдолд гэрчилгээг хүчингүй болгох хүсэлтийг гаргана. Захиалагчаас бусад төрлийн баталгаа гаргахыг шаардахгүй.

9.6.4 Хариуцагч талын төлөөлөл болон баталгаа

Хариуцагч тал нь захиалагчийн гэрчилгээг түүнийг нотлох зорилгоор ашиглана. Хэрэв:

- Хариуцагч тал нь захиалагчийн гэрчилгээнд итгэхийн өмнө захиалагчийн гэрчилгээг бий болгосон Гэрчилгээний байгууллагын гэрчилгээний бодлого болон журамтай танилцсан байна.
- Гэрчилгээг зөвхөн зөвшөөрөгдсөн зориулалтын дагуу хэрэглэнэ.
- Хариуцагч тал нь сэтгэл хангалуун байх үүднээс гэрчилгээний хүчинтэй байдлыг шалгана.

9.6.5 Бусад оролцогчийн төлөөлөл болон баталгаа

Нөхцөл байхгүй.

9.7 Баталгааг цуцлах

Гэрчилгээний байгууллага нь гэрчилгээний бодлого болон журамд заагдсаны дагуу хэрэглэгчдийг таних програм хангамж болон үйлдлүүдийг хэрэглэнэ. Хэдий тийм боловч энэ нь мэдээллийн үнэн зөвийг батлах эцсийн арга биш. Мөн Гэрчилгээний байгууллага нь хэрэглэгч болон харилцагч талуудын хувийн түлхүүрийн нууцлал ба түүнийг буруугаар ашиглах, хариуцагч талууд хоорондоо харьцахдаа гэрчилгээг ашиглахад хариуцлага хүлээхгүй.

Хариуцагч талууд гэрчилгээг зориулалтын бусаар өөр ямар нэгэн байдлаар ашиглавал бүх хариуцлага болон эрсдэлийг өөрсдөө даана.

9.8 Үүргийн хязгаарлалтууд

Монгол улсын хуульд тусгайлан заагаагүй тохиолдолд Гэрчилгээний байгууллага харилцагч тал гэрчилгээг гэмтээх, хүчинтэй гэрчилгээг хүлээн авахгүй байх, хүчингүй болсон гэрчилгээг ашиглах зэрэг тохиолдолд ямар нэгэн үүрэг хүлээхгүй. Мөн Гэрчилгээний байгууллага нь захиалагчийн гэрчилгээ авахыг хүссэн хүсэлт эвдэрсэн, гэрчилгээг хүчингүй болгох хүсэлтийг Гэрчилгээний байгууллага гаргасан, гэрчилгээний бодлого болон журмын баримт бичгийн харьцаж буй бүртгэлийн нэгж баталгаажуулсан тохиолдлуудад ямар нэгэн үүрэг хүлээхгүй.

9.9 Нөхөн төлбөр

Нөхцөл байхгүй.

9.10 Цаг хугацаа болон зогсоох

9.10.1 Нөхцөл

Энэ баримт бичиг нь Гэрчилгээний байгууллагын веб хуудсан дээр тавигдсан өдрөөс эхлэн хүчин төгөлдөр болно. Баримт бичгийг дуусах хугацааг заахгүй.

9.10.2 Таслан зогсоох

Энэхүү гэрчилгээний бодлого болон журам нь дараагийн шинэ хувилбар гартал хүчинтэй байна.

9.10.3 Таслан зогсоосноос үүсэх үр нөлөө.

Гэрчилгээний бодлого болон журмын баримт бичиг хүчингүй болохоос өмнө олгогдсон хамгийн сүүлчийн гэрчилгээний хугацаанаас хойш 5 жилийн дотор энэхүү баримт бичгийг олж авч болохоор хадгална.

9.11 Оролцогчдын хувийн тэмдэглэл болон харилцаа.

Гэрчилгээний байгууллага болон түүний итгэмжлэгдсэн бүртгэлийн нэгжүүдийн хоорондох бүх эмайл тоон гарын үсгээр баталгаажсан байна. Аливаа үйлдлийг хийж гүйцэтгэх хүсэлт бүр тоон гарын үсэг зурагдсан байна.

9.12 Нэмэлт өөрчлөлт

9.12.1 Нэмэлт өөрчлөлтийн үйл явц

Гэрчилгээний бодлого болон журамд оруулах нэмэлт өөрчлөлтийг 1.5.4 заалтад заасны дагуу хийж гүйцэтгэнэ. Найруулгыг сайжруулах, үг үсгийн алдааг засах нь нэмэлт өөрчлөлтөд хамаарахгүй.

9.12.2 Мэдэгдэл гаргах арга зам болон хугацаа.

Шинэчлэгдсэн гэрчилгээний бодлого болон журмыг хэрэгжиж эхлэхээс 2 долоо хоногийн өмнө Гэрчилгээний байгууллагын веб хуудсан дээр тавигдах ёстой. Гэрчилгээний байгууллага энэ тухай бүх хэрэглэгчид болон хариуцагч талуудад эмайлээр мэдэгдэнэ.

9.12.3 Гэрчилгээний байгууллагыг таних кодыг(OID) солих нөхцөл

Зайлшгүй шаардлагын улмаас OID-ийг өөрчилж болно. Өөрчлөх хүсэлтийг Гэрчилгээний байгууллагын ерөнхий менежер удирдлагын зөвлөлд танилцуулан зөвшөөрөл авснаар өөрчлөлтийг хийнэ.

9.13 Маргаан шийдвэрлэх хэлэлцээрийн зүйлс.

Гэрчилгээний бодлого болон журмаас гадуурх маргаантай асуудлыг Гэрчилгээний байгууллагын ерөнхий менежер шийдвэрлэнэ.

9.14 Хуулийн биелэлт

Гэрчилгээний байгууллага болон түүний үйл ажиллагаа нь Монголын хуулийн дагуу явагдана.

9.15 Хамааралтай хуулийн хэрэгжүүлэлт.
Гэрчилгээтэй холбоотой түүнийг хүсэх, шинээр олгох, ашиглах бүх үйл явц нь Монгол улсын хуульд нийцсэн байна.

9.16 Өөр бусад төрлийн заалтууд

9.16.1 Гэрээ хэлцлээр
Хамааралгүй.

9.16.2 Үүрэг даалгавар
Хамааралгүй.

9.16.3 Тусгаар байдал.
Гэрчилгээний бодлого болон журмын заалт нь Монгол улсын хууль (9.14 заалтыг харна уу), шүүх болон хуулийн байгууллагаас гаргасан тайлбартай зөрчилдвөл энэхүү зөрчилтэй хэсгийг нэн даруй баримт бичгээс хасах бөгөөд баримт бичгийн үлдсэн хэсэг нь хүчинтэй байх болно.

9.16.4 Албадлага (өмгөөлөгчийн хөлс эрхүүдийн татгалзагч)
Хамааралгүй.

9.16.5 Гэнэтийн аюул
Гэрчилгээний байгууллагын хяналтаас гадуурх үйл явдал болбол удирдах зөвлөл нэн яаралтай шийднэ.

9.17 Бусад заалтууд
Нөхцөлгүй.

10. Бусад зохицуулалт – Бүртгэлийн нэгж байгуулах, бүртгэлийн үйл ажиллагаа явуулах

10.1 Нийтлэг зүйл

10.1.1 Бүртгэлийн нэгж (БН) нь Тоон Гэрчилгээ авах, гэрчилгээг хүчингүй болгох, түдгэлзүүлэх өргөдлийг хүлээн авах, боловсруулах зорилгоор тусгай зөвшөөрөл эзэмшигчийн байгуулсан нэгж, эсхүл тусгай зөвшөөрөл эзэмшигчтэй гэрээ байгуулсан хуулийн этгээдийн байгуулсан нэгж байна. Гэрчилгээ авах өргөдлийг тусгай зөвшөөрөл эзэмшигчийн албан ёсны веб сайт, веб агуулахад байршуулсан байна. Өргөдөлд өргөдөл гаргагчийн овог нэр, бусад хувийн мэдээлэл, ажил, албан тушаал болон БН-ийн ашиглах бусад шаардлагатай мэдээллийг оруулна.

10.2 Шинэ Бүртгэлийн Нэгж байгуулах

10.2.1 Бүртгэлийн Нэгж байгуулахын тулд тусгай зөвшөөрөл эзэмшигчийн удирдах ажилтан зохих саналыг боловсруулж тусгай зөвшөөрөл эзэмшигчийн дээд удирдлагад өргөн барина. Хэрэв бүртгэлийн нэгжийг тусгай зөвшөөрөл эзэмшигчээс өөр байгууллага байгуулан ажиллуулах гэж байгаа бол удирдах ажилтны (Ерөнхий менежер, дэд захирлаас доошгүй албан тушаалтай) албан ёсны гарын үсэг, тамга бүхий албан бичгийг тусгай зөвшөөрөл эзэмшигчид хүргүүлнэ.

10.2.2 Бүртгэлийн нэгж бүр хоёроос доошгүй ажилтантай байна. Үүнд системийн зохицуулагч, БН-ийн эрхлэгч болон бусад ажилтан байж болно. Тусгай зөвшөөрөл эзэмшигчийн удирдлага, эсхүл тусгай зөвшөөрөл эзэмшигчтэй гэрээ байгуулсан хуулийн этгээдийн удирдлага дээрх ажилтнуудыг томилно.

10.2.3 Удирдлагын томилсон БН-ийн эрхлэгч БН-ийн бүх үйл ажиллагаа, удирдлагыг хариуцна.

10.2.4 БН-ийн эрхлэгч өөрийн тоон гарын үсгийн гэрчилгээ авах өргөдлийг доор дурдсан бусад баримт бичиг болон БН-тэй байгуулах тамга дарж гарын үсэг зурсан гэрээний хамт тусгай зөвшөөрөл эзэмшигчид хүргүүлнэ.

10.2.5 Өргөдөлд дараах баримт бичгүүдийг хавсаргана:

10.2.6 Гэрчилгээ эзэмшигчтэй хийх гэрээ

10.2.6.1 Иргэний ухаалаг үнэмлэхний нотариатаар баталгаажуулсан хуулбар (Тусгай зөвшөөрөл эзэмшигчийн гүйцэтгэх удирдлагатай биечлэн уулзаж өөрийгөө баталгаажуулахын зэрэгцээ ухаалаг үнэмлэхний хуулбарыг өгнө)

10.2.6.2 Хэрэв тусгай зөвшөөрөл эзэмшигчтэй гэрээ байгуулсан хуулийн этгээд БН байгуулж байгаа бол тухайн байгууллагын захирлын гарын үсэг, тамгатай албан тоот

10.2.6.3 Өргөдөлд хавсаргах 3х4 хэмжээний зураг

10.2.6.4 БН-ийн эрхлэгч Тусгай зөвшөөрөл эзэмшигчийн захиргаагаар дамжуулан гэрчилгээ олгох үйлчилгээ хүссэн өргөдлөө өгөх бөгөөд FIPS140-1/2 түвшин 2-т нийцсэн болон түүнээс дээш төвшний криптографын модулийн (ухаалаг карт/ етокен) гэрчилгээ авна. Гэрчилгээний үнийг БН байгуулж буй хуулийн этгээд төлнө.

10.2.6.4 Гэрчилгээний жишиг үнийг ГБ санал болгосноор ХХЗХтогтооно.

10.2.6.5 БН-ийн эрхлэгч, зохицуулагч болон ажилтан тусгай зөвшөөрөл эзэмшигчийн гэрчилгээжүүлэх ажиллагааны журам болон БН-тэй байгуулсан гэрээнд тусгасан үүргүүдийг биелүүлж ажиллана.

10.3 Бүртгэлийн нэгжид тавигдах шаардлага

10.3.1 Монгол Улсын “Цахим гарын үсгийн тухай” хууль, тусгай зөвшөөрөл эзэмшигчийн гэрчилгээжүүлэх ажиллагааны журамд заасан чиг үүрэг, үйл ажиллагааг хэрэгжүүлэхийн тулд БН-ийг тусгай зөвшөөрөл эзэмшигчийн бүтцэд юм уу тусгай зөвшөөрөл эзэмшигчтэй гэрээ байгуулсан хуулийн этгээдийн бүтцэд байгуулна. БН-д дараах дэд бүтцийг бүрдүүлсэн байна:

10.3.1.1 БН-ийн эрхлэгч, зохицуулагч хэмээн нэрлэгдэх хоёр албан тушаалтан;

10.3.1.2 Нэг туслах ажилтан, нарийн бичгийн дарга (заавал биш);

10.3.1.3 Ажилдаа ашиглах ухаалаг карт уншигч юм уу зохих порт бүхий ширээний хоёр компьютер, Администраторын ашиглах компьютерт БН-ийн онлайн үйлчилгээг хангахуйц БН-ийн зориулалттай хэрэглээний програм хангамж суулгасан байна.

10.3.1.4 БН-ийн үйлчилгээнд хандахад зориулсан Интернетийн холболт, дотоод сүлжээ;

10.3.1.5 Өгөгдлийн нөөц хуулбар агуулсан, БН-ийн хэрэглээний програм бүхий нөөц компьютер нэг ширхэг;

10.3.1.6 Үйлчлүүлэгчийн мэдээллийг нууцлан хадгалах боломжтой тээгч, түүнийг хадгалах цоож түгжээ бүхий сейф - Төвлөрсөн серверээс онлайнаар https протокол ашиглан үйлдэж байгаа тохиолдолд энэхүү нөхцөл шаардлагагүй.

10.3.1.7 БН-ийн өгөгдлийн нөөц хуулбар хийх шийдэл, механизм, тээгч - Төвлөрсөн серверээс онлайнаар https протокол ашиглан үйлдэж байгаа тохиолдолд энэхүү нөхцөл шаардлагагүй.

10.3.1.8 Тоон гэрчилгээ хүссэн үйлчлүүлэгчийг шалган баталгаажуулах журам, Өөрийн хяналт, аудитын тайлан гаргах журам болон мэдээллийн аюулгүй байдлыг хангах бодлого, дотоод бусад журмууд;

10.3.1.9 Үйлчлүүлэгчийн тухай өгөгдлийг 7-оос доошгүй жил аюулгүй архивлан хадгалах шийдэл;

10.3.2 Техник хангамж/ Програм хангамжийн шаардлага:

10.3.2.1 Хоёр ширхэг ширээний компьютер;

10.3.2.2 Үйлдлийн систем: Ажлын шаардлага хангасан;

10.3.2.3 Администраторын компьютерт БН-ийн хэрэглээний програм суулгасан байна - Төвлөрсөн серверээс онлайнаар https протокол ашиглан үйлдэж байгаа тохиолдолд энэхүү нөхцөл шаардлагагүй.

10.3.2.4 Процессор: Ажлын шаардлага хангасан;

10.3.2.5 RAM: Ажлын шаардлага хангасан;

10.3.2.6 Тээгчийг унших драйверуудтай;

10.3.2.7 Интернет холболт;

10.3.2.8 Орчин үеийн шаардлага хангасан Иргэний ухаалаг үнэмлэх уншигч болон зохих портуудтай;

10.4 Бүртгэлийн нэгжид үүсгэж хөтөлж байх тайлан, бичлэг

10.4.1 Үйлчлүүлэгчийн гаргасан өргөдөл. Өргөдөл нь бүрэн бөглөгдсөн, гарын үсэг зурсан, БН-ийн эрхлэгч хянаж баталгаажуулсан байна.

10.4.2 Гэрчилгээг хүчингүй болгох, түдгэлзүүлэх өргөдөл.

10.4.3 Тусгай зөвшөөрөл эзэмшигчтэй байгуулсан гэрээний хуулбар.

10.4.4 Үйлчлүүлэгчтэй байгуулсан гэрээнүүд.

10.4.5 Гэрчилгээний ангиллын дагуу үйлчлүүлэгчийн хувийн мэдээллийг шалгахад зайлшгүй шаардлагатай баримт бичиг, журмууд.

10.4.6 БН-д ашиглагдаж буй тооцоолох төхөөрөмж, компьютерийн тохируулгын тайлан.

10.4.7 Тусгай зөвшөөрөл эзэмшигчийн програм хангамж, серверүүдээс үүсгэсэн төрөл бүрийн баримт бичлэгийн нөөц хуулбарууд.

10.4.8 Үйлчлүүлэгчийн иргэний ухаалаг үнэмлэх болон хэрэглэгчийн ID-ийн софт хуулбарууд.

10.4.9 Үйлчлүүлэгчээс хүлээн авсан санхүүгийн төлбөрийн баримт бичгүүд.

10.4.10 Тусгай зөвшөөрөл эзэмшигчид төлбөрийн шилжүүлсэн баримт бичгүүд.

10.4.11 Хэрэглэгчийн ID болон хандалтын эрх хүлээн авсан баталгаажуулалт.

10.4.12 Үйлчлүүлэгч, хэрэглэгчтэй харилцаж байсан харилцаа, цахим захиа, товч мэдээллийн хуулбар.

10.4.13 БН-ийн ажлын компьютерууд дээр суулгасан системийн болон хамгаалалтын програм хангамжийн нарийвчилсан үзүүлэлт, тохируулгын тодорхойлолт.

10.4.14 БН-ийн ажлын компьютерууд дээр суулгасан хамгаалалтын програмын нарийвчилсан тодорхойлолт, тохируулгын тодорхойлолт.

10.4.15 Хувийн түлхүүр, гэрчилгээгээ алдсан, нууцлалаа алдсан үйлчлүүлэгчийн тухай баримт, бичлэгүүд.

10.4.16 Аудит, хяналтын ул мөр, нотолгоо агуулсан аливаа баримт, бичлэгүүд.

10.5 БН-ийн даган мөрдөх үндсэн журмууд

10.5.1 БН-ийн бүртгэл хийх журам

10.5.1.1 Бүртгэлийн нэгж хэрэглэгч, үйлчлүүлэгчийн өргөдлийг хүлээн авах, бүртгэх, тусгай зөвшөөрөл эзэмшигчид дамжуулах, гэрчилгээнд гарын үсэг зуруулах өргөдлийг нь дамжуулах, гэрчилгээг хүргүүлэх, гэрчилгээг хүчингүй болгох, түдгэлзүүлэх өргөдлийг хүлээн авах, хадгалах санд оруулах, вебэд байршуулах үйл ажиллагааны дэгийг тусгай зөвшөөрөл эзэмшигчийн гэрчилгээжүүлэх ажиллагааны журамд тодорхойлсон байна.

10.5.2 Баримт, бичлэг тайланг архивлан хадгалах

10.5.2.1 Үйлчлүүлэгчийн гаргасан өргөдлүүд, гэрчилгээг хүчингүй болгох, түдгэлзүүлэх өргөдлүүд болон үйлчлүүлэгчийг шалган баталгаажуулахтай холбоотой мэдээллийг хамгийн багадаа 7 жил хадгална.

10.5.2.2 БН-ийн үйл ажиллагаа, үйлчлүүлэгчийн өргөдөл, баталгаажуулалт, адилтгал, зөвшөөрөл олгохтой холбоотой бүх мэдээлэл, гэрээнүүдийг тусгай зөвшөөрөл эзэмшигчийн зөвшөөрөлгүйгээр задлах, нийтэд дэлгэхийг хориглоно.

10.5.2.3 Хяналт шалгалт, аудитын мэдээлэл болон програм хангамжийн үүсгэсэн аудитын тайлан мэдээллийг зөвшөөрөлгүй үзэх, өөрчлөх, устгахаас хамгаалсан байна.

10.5.3 Хог хаягдлыг устгах

10.5.3.1Тусгай зөвшөөрөл эзэмшигч болон БН-ийн үйл ажиллагаатай холбоотой аливаа баримт бичиг, цахим мэдээллийг тусгай зөвшөөрөл эзэмшигчийн зөвшөөрөлгүйгээр устгахыг хориглоно. Эдгээр баримт бичиг, мэдээлэл,

тайлан мэдээллийг тусгай зөвшөөрөл эзэмшигчийн зөвшөөрлөөр дахин ашиглах боломжгүйгээр устгана.

10.5.4 Баримт бичгийн аюулгүй байдал

10.5.4.1 Тусгай зөвшөөрөл эзэмшигч болон БН-ийн үйл ажиллагаатай холбоотой аливаа баримт бичгийн аюулгүй байдлыг хангах үүднээс нууц шифрлэлт бүхий цоожтой сейфэнд хадгална. Цахим баримт бичгийг компьютер дээр шифрлэн хадгална. БН-ийн зохицуулагч баримт бичгийн хадгалалтыг хариуцна.

10.5.5 Тээгч болон баримт бичгийн удирдлага

10.5.5.1 Нууц, албаны мэдээлэл агуулсан аливаа тээгч, баримт бичгийг нууц шифрлэлт бүхий цоожтой сейфэнд хадгална.

10.5.5.2 БН-д ирж буй болон гарч буй бүх тээгч, баримт бичгийг БН-ийн зохицуулагч хянаж зөвшөөрнө.

10.5.5.3 Бүх тээгч баримт бичгийн хэмжээ, агуулгыг гаднаас нь адилтгах боломжтой байна. Хэрэв боломжтой бол баримт бичгийн өргөтгөл, дотоод тэмдэглэгээг хэрэглэнэ.

10.5.6 Тээгч болон Баримт бичгийг зөөвөрлөх

10.5.6.1 Тусгай зөвшөөрөл эзэмшигч болон БН-ийн хооронд зөөвөрлөж буй аливаа тээгч, компьютерийн диск, цаасан баримт бичгийн шилжилт, хөдөлгөөнийг зохих ёсоор бүртгэж хянаж байх ёстой.

10.5.6.2 Тусгай зөвшөөрөл эзэмшигч болон БН-ийн хооронд аливаа тээгч/ баримт бичгийг тусгай зөвшөөрөл эзэмшигчийн зөвшөөрөлтэйгөөр аюулгүй шилжүүлэх дэг, журмыг хэрэгжүүлсэн байна.

10.5.6.3 Тусгай зөвшөөрөл эзэмшигч болон БН-ийн хооронд шилжүүлсэн аливаа тээгч/ баримт бичгийг цоожтой, хамгаалалттай сав, сейфэнд хадгална.