НТДБ, ТООН ГАРЫН ҮСЭГ: Тэдгээр нь хэрхэн ажилладаг вэ?

Хэрэглэгчдэд зориулсан гарын авлага

Боловсруулсан:

“МонПасс СА” ХХК ГЭРЧИЛГЭЭ ОЛГОХ БАЙГУУЛЛАГА
Хаяг: Монгол улс, Улаанбаатар хот, БЗД, 1 хороо,
Токиогийн гудамж, НИСОРА цамхаг 702 тоот
Утас: +976 76103286 | Факс: +976 76113286
И-Мэйл: info@monpass.mn | Веб сайт: www.monpass.mn

Зориулалт	Огноо	Хувилбар
Хэрэглэгч	2016.05.03	1.0

Агуулга

1. УДИРТГАЛ

Өнөөдөр МТ-ийн зөвлөхүүд болон мэргэжилтнүүдэд тулгарч буй томоохон сорилтуудын нэг нь шинээр болон тэргүүлэх технологийн талаарх мэдлэгийн түвшингээ байнга сайжруулахад оршиж байна. Бид мэдлэгээ байнга дээшлүүлж чадсанаар нийлүүлэгчид болон үйлчлүүлэгчийн дээд зэргийн сэтгэл ханамжийг хангаж чадна. Үүний үр дүнд бид хэрэглэгч танд дараах боломжуудыг бий болгож байдаг:

- Бизнесийн асуудлын талаарх бидний мэдлэг та бүхний хэлэлцдэг асуудал болон хувирна;
- Та өөрийн зорилго, зорилтуудаа шийдэхдээ технологийн шилдэг шийдлүүдийг ашиглана;
- Танд бизнесийн багагүй өгөөж авчирна;
- Янз бүрийн хязгаарлалтыг бууруулах боломж олгоно.

Өнөө үед тоон гарын үсгийн гэрчилгээ (ТГҮГ), нийтийн түлхүүрийг (НТ) нийтээрээ ашиглах болсон. ТГҮГ, НТ-тэй холбоотой олон шинэ стандарт болон арга техник, хэрэглээ бий болсоор байна. Гэтэл бид үүнийг чухам юу болох, хэрхэн ашиглах талаар мэддэг билүү? Тиймээс бид эдгээр нь юу болох, хэрхэн ажилладаг, яаж ашигладагийг мэдэх хэрэгтэй. Энэ танилцуулгад бид нийтийн түлхүүрийн шифрлэлт болон тоон гарын үсэг хэрхэн ажилладагийг тайлбарласан. Энэ танилцуулга нь Нийтийн түлхүүрийн дэд бүтэц (НТДБ-PKI) хэмээх өргөн ойлголтыг ойлгох эхлэлийн цэг байх болно.

Нийтийн түлхүүр гэж юу вэ?

Нийтийн түлхүүр гэдэг нь криптограф механизмын нэг чухал ойлголт. Тэгш хэмт криптограф түлхүүр, нийтлэг нууц, нууц (хувийн) түлхүүр гэсэн криптографын механизмуудаас түүнийг ялгах зорилгоор НТ гэж нэрлэгдсэн. Тэгш хэмт криптограф түлхүүр гэдэг нь ижил түлхүүр ашиглан мэдээллийг шифрлэн хувиргах болон шифлэлтийг буцаан тайлахад ашиглагддаг механизм юм. Энэ нь бид хаалгыг ижил түлхүүрээр цоожлоод буцаагаад онгойлгохтой адил хялбар ойлголт.

Тэгвэл нэг түлхүүр нь шифрлэдэг, нөгөө түлхүүр нь задалдаг, тэгш бус хоёр өөр хос түлхүүр ашигладаг өөр нэг концепцийг нийтийн түлхүүр гэдэг ойлголт төлөөлдөг. Энэ нь тэгш хэмт криптограф түлхүүрийн шийдлээс илүү давуу талтай маш үхаалаг шийдэл-концепци юм. Тухайлбал:

• Түлхүүрийн хялбархан түгээж, тарааж болно

• Тоон гарын үсэг зурж болно

• Урт хугацааны шифрлэлт хийж болно.

1.1 Тодорхойлолт

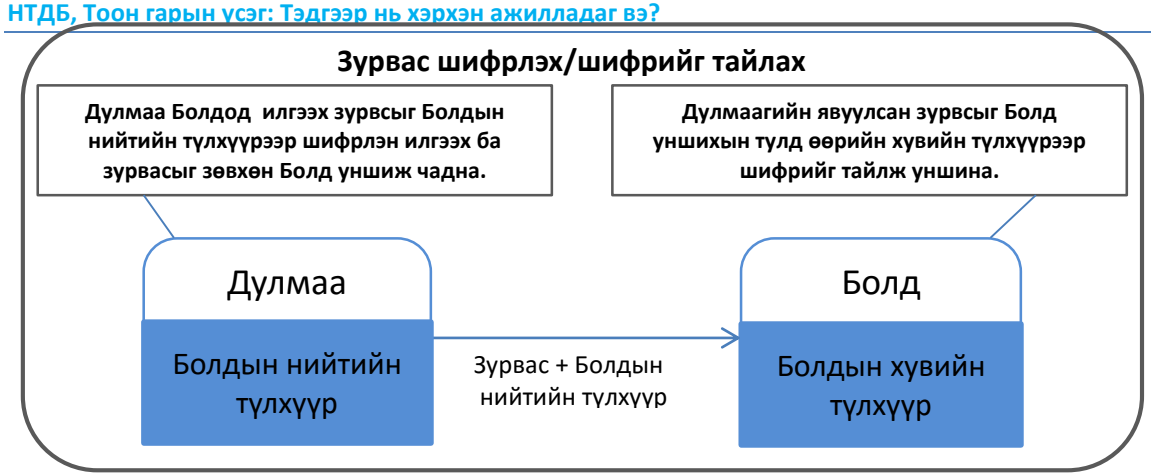
Нийтийн түлхүүр, хувийн түлхүүр хэмээх тэгш бус (хоёр өөр) хос түлхүүр ашигладаг криптографын аргыг Нийтийн Түлхүүрийн арга гэж нэрлэдэг. Нийтийн түлхүүр болон Хувийн (нууц) түлхүүр тусгай математик хамаарлаар холбогдсон байна. Нийтийн түлхүүрийг ашиглан шифрлэдэг бол хувийн түлхүүр ашиглан задалдаг. Нийтийн түлхүүр нь системийн бүх хэрэглэгчдэд нээлттэй, үнэгүй татаж авах боломжтой байх ба цахим гарын үсгийг шалгах болон шифрлэлт хийхэд зориулагдсан байдаг. Харин хувийн түлхүүрийг эзэмшигчээс өөр хэн ч мэдэх боломжгүй байх ёстой. Нийтийн түлхүүрийг ашиглан мэдээллийг шифрлэдэг бол зөвхөн түүнд хамааралтай хувийн түлхүүрээр уг мэдээллийг задлах боломжтой байна. Эсрэгээр мэдээллийг хувийн түлхүүрээр шифрлэсэн бол зөвхөн түүний нийтийн түлхүүрийг ашиглан задлана. Энэ чанарыг ашиглан шифрлэлт болон тоон гарын үсгийг хэрэгжүүлсэн байдаг. Шифрлэлт болон Тоон гарын үсгийн зарчмуудыг Зураг1, Зураг2-т үзүүлэв.

1.2 Шифрлэлт болон задлалт

Шифрлэлт – энэ нь зөвхөн илгээгч болон хүлээн авагч унших, харах боломжтойгоор мэдээллийг кодлон хувиргах арга юм. Шифрлэлтийн зорилго нь – Нууцлал.

Жишээ нь, Дулмаагаас Болдод Хувийн нууц зурвас илгээж байгаа үйл явцыг авч үзье.

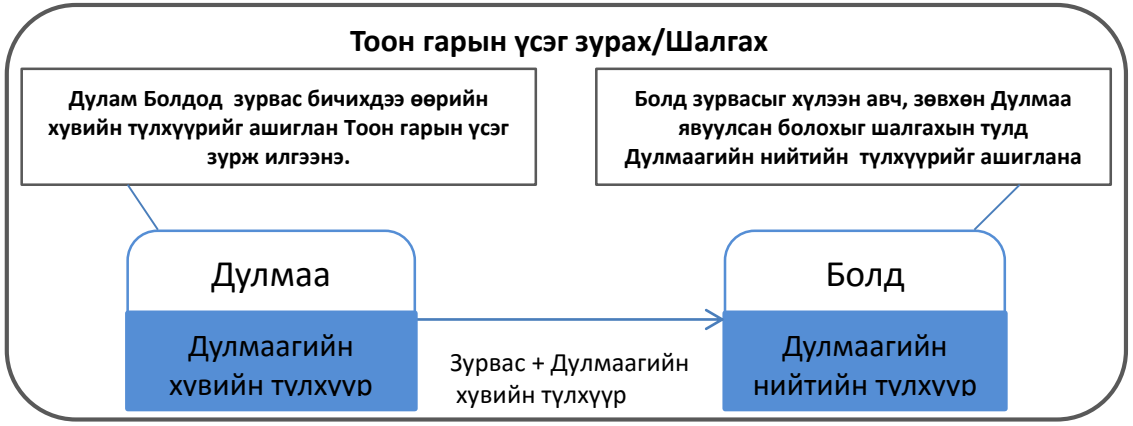
Дулмаа зурвасаа өөр хэн ч уншиж чадахааргүй шифрлэн илгээхийн тулд эхлээд Болдын нийтийн түлхүүрийг Гэрчилгээ Олгогч Байгууллагын веб сангаас татаж авах юмуу Болдоос э-мэйлээр хүлээн авна. Нийтийн түлхүүрийг хүн болгон харж болох тул Болд өөрийн нийтийн түлхүүрээ сүлжээгээр дамжуулан явуулж болно. Дуламд Болдын нийтийн түлхүүр байгаа учир уг түлхүүрийг ашиглан зурвасаа шифрлэн илгээнэ. Болд уг зурвасыг хүлээн аваад, өөрийн хувийн түлхүүрийг ашиглан шифрлэлтийг задалж уншина (Зураг 1).



Зураг 1. Шифрлэх болон задлах зарчим

Тоон гарын үсэг гэдэг нь мэдээллийг адилтган баталгаажуулах, өөрөөр хэлбэл уг мэдээлэл илгээсэн хүнээс ирсэн гэдгийг хөдөлбөргүй батлах харуулах механизм бөгөөд цаасан баримт дээр зурсан гарын үсэгтэй ижил хүчин төгөлдөр байдаг.

Жишээ нь, Дулам Болдод илгээж буй захидалдаа тоон гарын үсэг зурахыг хүсэж байна. Үүний тулд Дулам өөрийн хувийн түлхүүрийг ашиглан захидал мэдээллээ шифрлээд өөрийн нийтийн түлхүүрийг хавсарган Болдод илгээнэ (ихэвчлэн, нийтийн түлхүүрийг гарын үсэг зурсан зурвастай хамт хавсаргана). Хэрэв нийтийн түлхүүрийг хавсаргаагүй бол Болд Дуламын нийтийн түлхүүрийг ГОБ-ын веб сангаас татаж авна. Хэрэв Дуламын нийтийн түлхүүр уг захидлыг тайлж уншиж чадаж байвал захиаг Дулам илгээсэн гэдэг нь хөдөлбөргүй батлагдана. (Зураг 2)



Зураг 2 : Тоон гарын үсэг /баталгаажуулалтын зарчим

1.3 Тоон гарын үсгийг хэрхэн хялбаршуулах вэ?

Өмнөх хэсгүүдэд шифрлэх/код тайлах болон гарын үсэг зурах/шалгах, батагаажуулах үндсэн зарчмыг үзүүлсэн. Нууцлалыг баттай хангах, хөдөлбөргүй таньж баталгаажуулахын тулд Шифрлэлт, Тоон гарын үсгийг нэгэн зэрэг хослуулан ашиглаж болно. Өмнө дурьдсанчлан, тэгш бус хэмтэй түлхүүр ашиглан гарын үсэг зурахад цаг хугацаа харьцангуй их шаарддаг учир Тоон гарын үсэг зурахын тулд адилхан найдвартай, гэхдээ илүү хурдан өөр нэг арга ашигладаг. Үүнийг хэшлэх арга гэдэг. Хэшлэх явцад илгээх гэж буй мэдээллийн хосгүй, жижиг илэрхийлэл болох (хяналтын боловсронгуй дүнгийн битүүд мэт) мэдээллийн digest – товч илэрхийлэлийг (товчлол) үүсгэнэ. Хэшлэх алгоритм нь нэг чиглэлийн шифрлэлт юм, өөрөөр хэлбэл мэдээллийн digest –товч илэрхийлэлээс мэдээллийг гарган авч болдоггүй. Мэдээллийн digest – товч илэрхийлэл үүсгэж буй үндсэн шалтгаан нь:

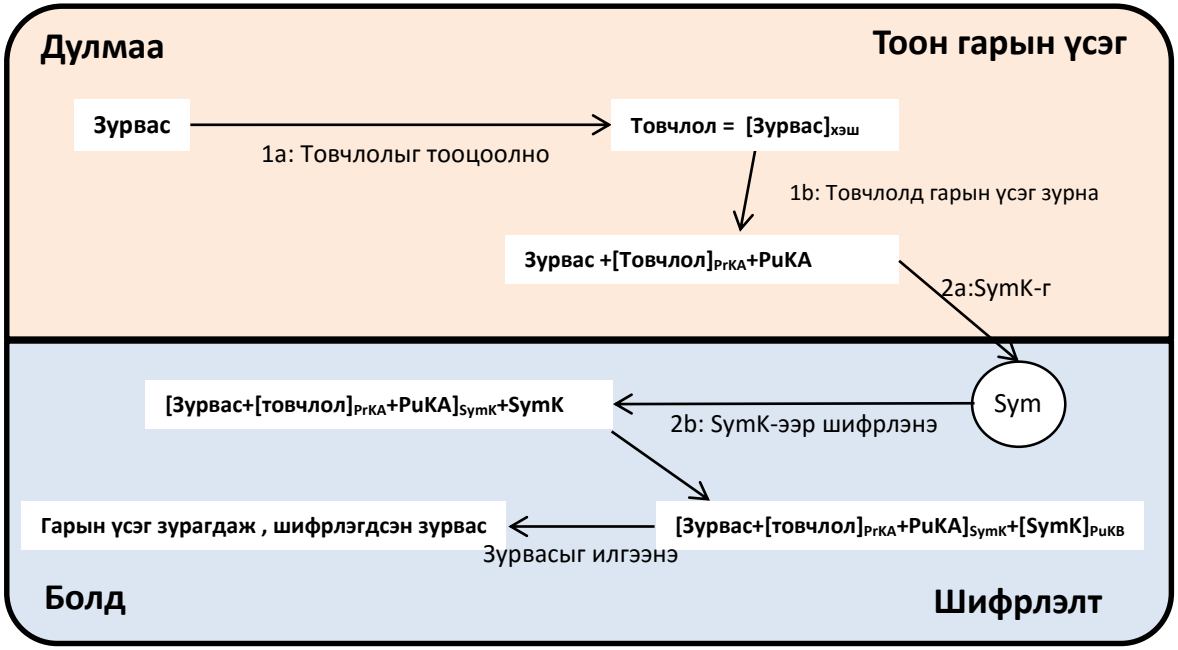
1. Илгээж буй мэдээллийн бүрэн бүтэн байдлыг хадгалах; ямар нэг өөрчлөлт оруулахад шууд илэрнэ;
2. Тухайн товч илэрхийллийг тоон гарын үсэг ашиглан шифрлэх;
3. Хэшлэх алгоритм нь шифрлэлтийн аливаа алгоритмаас хамаагүй хурдан байдаг

Дараах хэсгүүдэд мэдээллээ шифрлэх, гарын үсэг зурах, түүнийг задлах, шалгах үед ямар үйл явц явагддагийг авч үзье.

1.4.1 Мэдээллээ (зурвас) шифрлэх болон гарын үсэг зурах алхмууд

Доорхи зурагт Дулмаа мэдээлэлдээ (зурваст) гарын үсэг зураад шифрлэн илгээх үйл явцыг харуулсан.

Дулмаа гарын үсэг зурж шифрлэсэн мэдээллээ Болдод илгээх



Тайлбар:

- PrKA – Дуламын хувийн түлхүүр
- PuKA – Дуламын нийтийн түлхүүр
- PuKB – Болдын нийтийн түлхүүр
- SymK- Нэг удаагын тэгш хэмтэй түлхүүр
- Хэш – Хэшлэх алгоритм

Зураг 3 : Тоон гарын үсэг болон шифрлэлтийн үйл явц.

1. **Зурваст гарын үсэг зурах**:
   a) *Зурвасын товчлолыг шалгах*. Зурвасын товчлолыг шалгаж буй зорилго нь зурвас өөрчлөгдөөгүй гэдгийг бататгахад орших ба үүнийг зурвасын бүрэн бүтэн байдал гэдэг.
   b) *Гарын үсгийн зурах*. Гарын үсэг зурах гэдэг нь мөн чанартаа илгээгчийн хувийн түлхүүрийн (энэ тохиолдолд Дуламын) тусламжтай хийж буй шифрлэлт юм. Мөн гарын үсэг зурагчийн хэш алгоритмын нэр гарын үсэгт орно. Гарын үсэг зурагчийн нийтийн түлхүүр гарын үсэгт мөн хавсаргагдана. Энэ нь хүлээн авж буй хэн ч гэсэн гарын үсэг зурагчийн нийтийн түлхүүр болон хэш алгоритмыг ашиглан гарын үсгийг шалгаж шифрлэлтийг задлах боломжийг олгодог. Нийтийн түлхүүрийн шифрлэлт болон хэшлэх алгоритмийн онцлогийн дагуу зурвасын хүлээн авагч дараах нотолгоог баттай олж авна:
      I. Илгээгчийн хувийн түлхүүрээр товчлолыг шифрлэсэн байна.

II. Зурвасыг аливаа өөрчлөлтөөс хамгаалсан байна.

2. **Зурвасыг шифрлэх**. Шифрлэлт нь дараах гурван алхмаас бүрдэнэ:
   a) *Нэг удаагийн тэгш хэмтэй шифрлэх/задлах түлхүүр үүсгэх*. Тэгш бус хэмтэй түлхүүр ашиглан шифрлэх/задлах алгоритм нь том мэдээлэл, зурвастай ажиллахдаа ихээхэн хугацаа зарцуулдаг учир тэгш хэмтэй түлхүүрийн алгоритм хэрэглэдэг.
   b) *Зурвас шифрлэх*. Зурвасыг бүхэлд нь (зурвас болон гарын үсэг) SymK ашиглан шифрлэнэ (тэгш хэмтэй түлхүүрийг илүүд үздэг).
   c) *Тэгш хэмтэй түлхүүрийн шифрлэлт*. Хүлээн авагч зурвасыг задлахын тулд SymK-г мөн ашиглана. SymK нь зөвхөн хүлээн авагчид (Болд) хүртээмжтэй байх ёстой. SymK –ийг хүлээн авагчаас бусад хүнээс нуухын тулд хүлээн авагчийн нийтийн түлхүүрийг ашиглан шифрлэнэ. SymK нь зурвасаас хамаагүй бага хэмжээтэй учир (мэдээлэл нь маш урт байж болно) тэгш бус хэмтэй алгоритмийг бодвол үйл явц хурдан, үр дүнтэй байдаг.

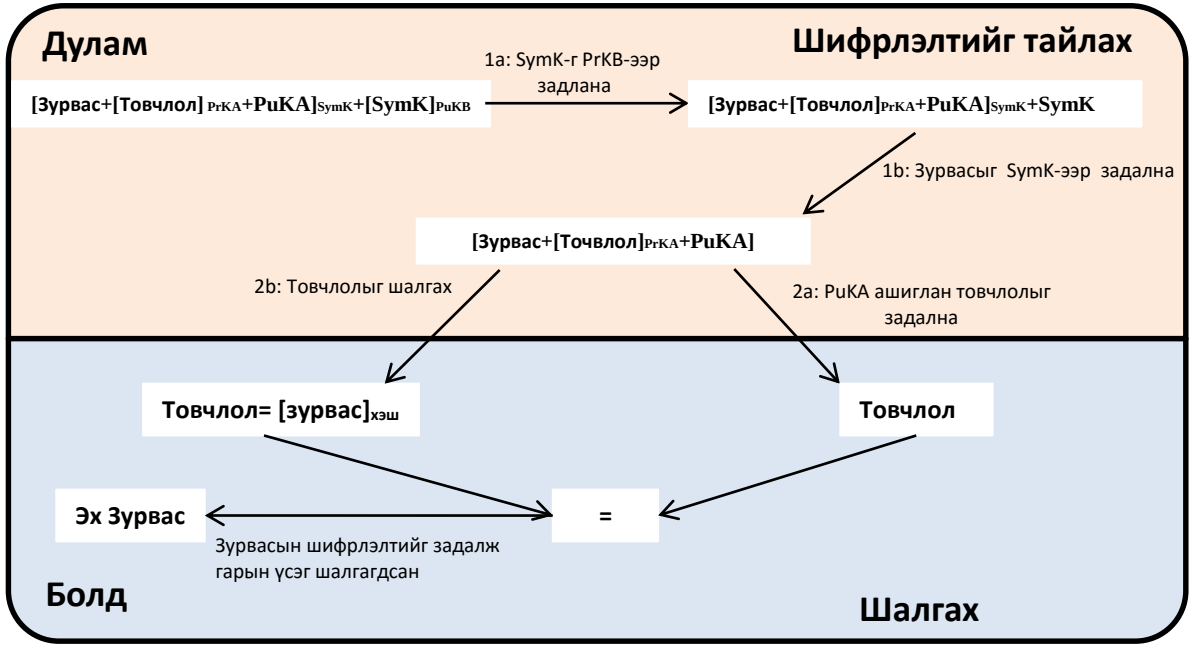
Хэрэв Дулам зурвасаа хэд хэдэн хүнд, тухайлбал Батад бас явуулахыг хүсвэл, Болд болон Батад тус бүрчлэн давтан илгээхийн оронд 2-р алхамыг Батад зориулан давтахад болно. Ингэснээр, Болд болон Батын хүлээн авч буй зурвас хоёуланд нь ижилхэн харагдана:

[Зурвас+[Товчлол-Digest]PrKA+PuKA]SymK+[SymK]PuKB+[SymK]PuK]. Болд болон Бат нэг ижил SymK - тэгш хэмт түлхүүр ашиглан зурвасын шифрлэлтийг задална.

1.4.2 Зурвасын гарын үсгийг шалгах болон шифрлэлтийг задлах (тайлах)

Болд Дуламаас хүлээж авсан зурвасыг задалж унших, гарын үсгийг шалгах үйл явцыг Дөрөвдүгээр зурагт харуулсан: $[Message+[Digest]_{PrKA}+PuKA]_{SymK}+[SymK]_{PuKB}$

$[Message+[Digest]_{PrKA}+PuKA]_{SymK}+SymK$



Тайлбар:

- PrKA – Дуламын хувийн түлхүүр
- PuKA – Дуламын нийтийн түлхүүр
- PuKB – Болдын нийтийн түлхүүр
- SymK- Нэг удаагын тэгш хэмтэй түлхүүр
- Хэш – Хэшлэх алгоритм

Зураг 4 : Шифлэлтийг задлах, гарын үсгийг шалган баталгаажуулах.

1. Шифрлэлтийг задлах.. Шифрлэлтийг задлахын тулд дараах алхмууд хийгдэнэ:

a) *Тэгш хэмтэй түлхүүрийн шифрлэлтийг задлах (тайлах).* Зурвасыг шифрлэхэд нэг удаагийн тэгш хэмт түлхүүр ашигласан байгаа. Энэ түлхүүрээ (SymK) хүлээн авагчийн (Болд) нийтийн түлхүүр ашиглан шифрлэсэн. Тиймээс зөвхөн Болд SymK түлхүүрийг задлалж түүнийгээ ашиглан зурвасыг тайлж унших боломжтой.

b) *Зурвасын (захидлын) шифрлэлтийг задлах (тайлах).* Зурвасыг (зурвас болон гарын үсэг) SymK түлхүүр ашиглан тайлж (задалж) уншина.

2. Гарын үсгийг шалгах. Гарын үсгийг шалгахын тулд дараахи 3 гурван алхмыг гүйцэтгэнэ:

a) *Зурвасын товчлолыг (digest) тайлах (задлах).* Илгээгчийн (Дулам) хувийн түлхүүр ашиглан товчлолыг агуулгыг шифрлэсэн. Тиймээс зурвасад агуулагдсан илгээгчийн нийтийн түлхүүр ашиглан товчлолыг задална (тайлна).

b) *Товчлолыг шалгах*. Хэш нь нэг чиглэлт үйл явц тул (жишээлбэл, товчлолоос зурвасыг шууд гарган авч болохгүй) илгээгчийн ашигласантай нэгэн ижил хэшлэх алгоритм ашиглан товчлолыг дахин шалгана.

c) *Товчлолыг харьцуулах*. а) - д заасны дагуу задалж гарган авсан товчлол болон б)-д заасны дагуу шалгаж буй товчлолыг хооронд нь харьцуулна. Хэрэв тэд ижилхэн байвал гарын үсэг шалгагдсан, үнэн зөв, зурвас өөрчлөгдөөгүй гэдэг нь батлагдана. Хэрвээ дээрх товчлолууд ижил бус байвал энэ нь дараах зүйлсийг илтгэнэ:

i. Зурвасыг илгээгч гарын үсгээ зурж баталгаажуулаагүй; эсхүл

ii. Зурвасыг өөрчилсөн;

iii. Дээрх 2 тохиолдолд зурвасыг буцаах нь зүйтэй.

1.4 Адилтгал болон Түлхүүрүүд

Шифрлэх/шифрлэлтийг тайлах болон тоон гарын үсэг зурах/шалгахад ашигладаг түлхүүрүүдийн (Дуламын болон Болдын) талаар бид үзлээ. Гэхдээ Дулам бол яг өөрөө мөн гэдгийг нь хэрхэн баталж, нотлох вэ? Мөн Дуламын шифрлэн илгээсэн зүйлийг зөвхөн Боб л харж байгаа гэдэгт нь хэрхэн итгэлтэй байх вэ? Түлхүүрийн жинхэнэ эзэн хэн бэ? Жишээ нь өөр этгээд Дуламын өмнөөс дүр эсгэн Болдруу зурвас илгээж байж болох юм. Зурвасыг илгээсэн этгээд яг Дулам мөн гэдгийг Болд баттай хэлж чадахгүй. Тэгвэл энэ асуудлыг тоон гарын үсгийн гэрчилгээ ашиглан шийддэг.

2. ГЭРЧИЛГЭЭ ГЭЖ ЮУ ВЭ?

Гэрчилгээ нь Нийтийн түлхүүр эзэмшигчийг таньж баталгаажуулах мэдээллийг агуулсан хэсэг мэдээлэл юм. Итгэлтэй хөндлөнгийн тал болох Гэрчилгээ Олгогч Байгууллага (ГОБ - Мон Пасс СА) тоон гарын үсгийн гэрчилгээг олгож гарын үсэг зураад найдвартай байдлаар хүргүүлдэг. Хөндлөнгийн итгэлтэй байгууллага болох ГОБ нь тухайн түлхүүрүүд Дулам, Болд нарынх мөн гэдгийг хөдөлбөргүй баталгаажуулж байдаг.

Гэрчилгээнд дараах мэдээлэл заавал орсон байдаг:

1) ГОБ-ийн мэдээлэл
2) Эзэмшигчийн мэдээлэл
3) Эзэмшигчийн нийтийн түлхүүр
4) Гэрчилгээний хүчинтэй хугацаа, дуусах огноо

5) Тухайн гэрчилгээнд ГОБ-аас зурсан тоон гарын үсэг
6) Бусад мэдээлэл.

Хүлээн авагч нийтийн түлхүүрээс гадна Гэрчилгээн дээр тулгуурлан тухайн гэрчилгээ яг ямар хүнд олгогдсон, хүчинтэй байгаа эсэхийг шалгаж, баталгаажуулж чадна. Тухайлбал:

1) Хэрэглэгчийн хэн болохыг хөдөлбөргүй тогтоох;
2) Гэрчилгээ нь хүчин төгөлдөр хэвээр байгаа эсэхийг шалгах;
3) Гэрчилгээнд тусгай зөвшөөрөл бүхий итгэлтэй ГОБ-ын гарын үсэг зурагдсан эсэх;
4) Эзэмшигч өөрөө гарын үсгээ зурсан эсэх, мэдээлэлд өөрчлөлт орсон эсэхийг шалгаж чадна.

Болд Дуламын гэрчилгээг шалгаснаар зурваст гарын үсэг зурахдаа яг Дуламын хувийн түлхүүр ашигласан байна гэдгийг нотолж болно. Тоон гарын үсэг эзэмшигч өөрийн хувийн түлхүүрийн маш чандлан нууцалж, хэн нэгэнд дэлгэхгүй, задлахгүй найдвартай хамгаалах ёстой. Хувийн түлхүүрээ нууцлан хамгаалж чадсанаар тухайн үйлдлийг үл татгалзах байдлаар хэрэгжүүлж чадна.

Гэрчилгээнд ГОБ гарын үсэг зурсан байдаг тул тэдгээрийг өөрчлөх боломжгүй болдог.

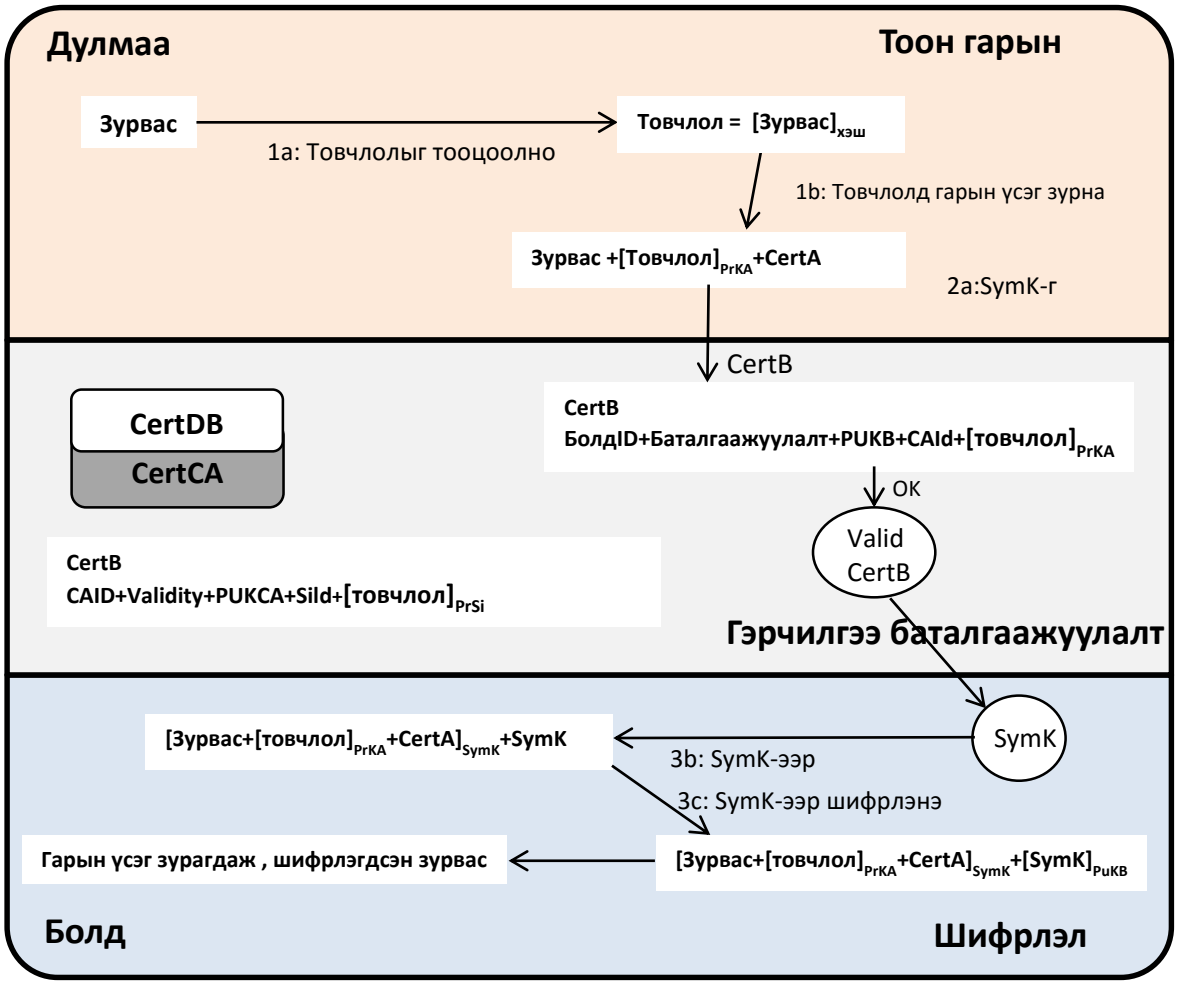
2.1 Гэрчилгээг шалган баталгаажуулах үйл явц

Дулам зурвасаа шифрлэн Болдруу илгээхдээ Болдын гэрчилгээг ашиглана. Тэрээр Болдын гэрчилгээнд агуулагдаж буй нийтийн түлхүүрийн ашиглахын өмнө Болдын гэрчилгээг шалган баталгаажуулахын тулд дараах алхмуудыг гүйцэтгэж болно:

1) Болдын гэрчилгээний хүчинтэй хугацаа;
2) Гэрчилгээ Болдод хамаарагддаг эсэх;
3) Болдын гэрчилгээнд өөрчлөлт орсон эсэх;
4) Гэрчилгээнд ГОБ гарын үсэг зурсан эсэх .

Дараах зурагт дээрх үйл явцыг харуулсан.

Дулам гарын үсэг зурж шифрлэсэн зурвасыг Болдод илгээж байна



Зураг 5: Гарын үсэг, шифрлэлт, түүнийг шалгах

Тайлбар:

- PrKA – Дуламын хувийн түлхүүр
- PrCA – ГОБ-ын хувийн түлхүүр
- PrSi – ГОБ-ын гэрчилгээнд гарын үсэг зурагчийн хувийн түлхүүр
- PuCA – ГОБ-ын нийтийн түлхүүр
- PuKB – Болдын нийтийн түлхүүр
- CertA – Дуламын гэрчилгээ
- CertB – Болдын гэрчилгээ
- CertCA – ГОБ-ын гэрчилгээ
- SymK- Нэг удаагын тэгш хэмтэй түлхүүр
- Хэш – Хэшлэх алгоритм
- БолдID – Болдын хосгүй дугаар
- CAId – ГОБ-ын хосгүй дугаар
- SiID – ГОБ-ын гэрчилгээнл гарын үсэг зурагчийн хосгүй дугаар
- Validity – Гэрчилгээний хүчинтэй хугацаа

Зураг 5-д зураг 3-д үзүүлсэн үйл явц дээр гэрчилгээг шалган баталгаажуулах үйл явцыг нэмсэн. Зөвхөн гэрчилгээг шалган баталгаажуулахад шаардлагатай талбарыг үзүүлсэн.

Болдын CertB гэрчилгээнд агуулагдаж буй PuKB нь Болдод яг хамааралтай бөгөөд хүчинтэй байгаа гэдэгт Дулам итгэлтэй байхыг хүсэж байна.

- Дулам ID талбараас Болдын адилтгалын мэдээллийг агуулсан ID-г хайж олно. Аль нь Бобын ID вэ. Үнэн хэрэгтээ энэ гэрчилгээ Болдод хамаарч байгаа гэсэн төсөөлөл Дуламд байгаа.
- Дараа нь тэр шалгах талбарыг нягталснаар гэрчилгээний мэдээллүүдийг олж үзнэ.
- Эцэст нь ГОБ-ын нийтийн түлхүүр (CertCA дахь PuKCA) ашиглан Болдын гэрчилгээн (CertB) дээрх гарын үсгийг нь шалгаснаар гэрчилгээ үнэхээр Болдынх мөн эсэхийг баталгаажуулна. Хэрвээ CertB дээрх гарын үсэг зөв (OK) гэж гарч ирж байгаа бол:
  a) Болдын гэрчилгээ нь итгэлтэй ГОБ-аас олгогдсон;
  b) Болдын гэрчилгээ бүрэн бүтэн, ямар нэг өөрчлөлт ороогүй болох нь баталгаатай;
  c) Болдын хувийн адилтгалын мэдээлэл баталгаатай, гэрчилгээн дахь нийтийн түлхүүр нь гарцаагүй Болдод хамаарагддаг бөгөөд хүчинтэй байна

гэдэг нь нотлогдож байна. Тиймээс Дуламын шифрлэж илгээсэн зурвасыг зөвхөн Болд түүний задлан уншиж чадна гэдэгт итгэлтэй байж болно. Болд ч Дуламын гарын үсгийг шалгахын өмнө түүний гэрчилгээг ийм замаар нягталж нотолж болно.

3. НИЙТИЙН ТҮЛХҮҮРИЙН ДЭД БҮТЭЦ (PKI) ГЭЖ ЮУ ВЭ?

Нийтийн түлхүүрийн дэд бүтэц (НТДБ) гэдэг нь хос түлхүүр болон гэрчилгээг удирдах, үр дүнтэйгээр ашиглах боломжийг хангаж буй програм хангамж, техник хангамж, дэг журам, хүмүүсийн нэгдэл юм. НТДБ-ийн үндсэн цөм нь Гэрчилгээ Олгох Байгууллага (ГОБ) байдаг. Төрөөс тусгай зөвшөөрөл авсан, итгэлтэй энэ байгууллага нь “Мон Пасс СА” ГОБ юм. Тиймээс НТДБ (Мон Пасс СА) -ийн хүрээнд түлхүүр болон гэрчилгээг хэрхэн удирддагийг авч үзье.

3.1 Түлхүүр болон гэрчилгээний удирдлага

Түлхүүр болон гэрчилгээний удирдлага гэдэг нь түлхүүр болон гэрчилгээг үүсгэх, дэмжих, хамгаалах цогц үйл ажиллагаа юм. НТДБ (Мон Пасс СА) -ийн хүрээнд хэрэгждэг үндсэн удирдлагуудыг дараах хэсэгт тодорхойлсон:

1) **Түлхүүр болон гэрчилгээг үүсгэх:** Хос түлхүүрийн хурхэн үүсгэх вэ? Хэрэглэгчдэд гэрчилгээ хэрхэн олгох вэ? Хэрэглэгч хос түлхүүр үүсгэх, гэрчилгээ авах хүсэлт үүсгэхэд нь НТДБ (Мон Пасс СА) програм хангамж юмуу тусгай хэрэгслээр хангах замаар дэмжлэг үзүүлдэг. Үүнээс гадна хэрэглэгчийг адилтгах, шалгах, таньж баталгаажуулах дэг журмыг нэвтрүүлсэн байна.

2) **Хувийн түлхүүрийн хамгаалалт**: Хэрэглэгч өөрийн хувийн түлхүүрийг төрөл бүрийн эрсдлээс хэрхэн хамгаалах вэ? Шифрлэх, гарын үсгийг шалгахад ашигладаг учир тоон гарын үсгийн гэрчилгээ, нийтийн түлхүүрийг нийтэд нээлттэй байршуулдаг. Харин хувийн түлхүүрийг гарын үсэг зурах, шифрийг тайлах, задлахад ашигладаг учир нууц, хамгаалагдсан байдлаар хадгалах ёстой. Тиймээс нууц үгээ хамгаалахдаа найдвартай, хүчтэй нууц үгийн механизм заавал ашигласан байх ёстой.
3) **Гэрчилгээг хүчингүй болгох**: Хэрэглэгчийн хувийн түлхүүр алдагдсан, ажилтан ажлаасаа гарсан, гэрчилгээний хугацаа дууссан тохиолдолд гэрчилгээг зүй бусаар ашиглахаас хэрхэн хамгаалах вэ? Гэрчилгээ хүчинтэй байгаа эсэхийг хэрхэн мэдэх вэ? НТДБ (Мон Пасс СА) -д гэрчилгээг хүчингүй болгох хэрэгсэл, мэдээлэх суваг, аргуудыг байнга бэлэн байлгах ёстой. Нэгэнт хүчингүй болсон гэрчилгээг Хүчингүй Гэрчилгээний Жагсаалтад (ХГЖ) оруулж нийтэд ил тод байлгана. Хүчингүй гэрчилгээний жагсаалтыг шалгах шийдлийг нийтэд санал болгосон байхаас гадна хүчингүй гэрчилгээ ашиглах оролдлогыг автоматаар хаадаг байна.
4) **Түлхүүрийг нөөцлөн хуулбарлах болон сэргээх**: Хэрэглэгч хувийн түлхүүрээ алга болгосон тохиолдолд шифрлэгдсэн файлуудаа хэрхэн задлах вэ? Хэрэв хувийн түлхүүрээ нөөцлөн хуулбарлаагүй бол нийтийн түлхүүрээр шифрлэсэн бүх зурвас, захидал, мэдээлэл, бичиг баримтуудыг дахин задлах, тайлах боломжгүй болно. Тиймээс хувийн түлхүүрийг нөөцлөн хуулбарлах, сэргээх шийдлийг НТДБ (Мон Пасс СА) хэрэглэгчдэд санал болгодог, түүнийг хэрэглэгч ашиглах боломжтой байх ёстой.
5) **Түлхүүр болон гэрчилгээг шинэчлэх**: Гэрчилгээний хугацаа дуусах дөхсөн бол яах вэ? Түлхүүр болон гэрчилгээ нь тодорхой хугацаатай байдаг. НТДБ (Мон Пасс СА) гэрчилгээний хугацаа дуусах өдрийг сануулж, түүнийг шинэчлэх механизмыг санал болгосон байх ёстой.
6) **Түлхүүрийн түүхийн удирдлага**: Түлхүүрээ хэд хэдэн удаа шинэчлэсний дараа файлуудыг задлахын тулд аль түлхүүрээ ашиглах вэ? гэдэг асуудал гарч ирдэг. Гэрчилгээ, түлхүүрээ шинэчлэх бүрт шинээр хос түлхүүр үүсгэдэг. Файлууд нь өмнөх нийтийн түлхүүрээр шифрлэгдсэн байдаг учир зөвхөн холбогдох хувийн түлхүүрээр задалж болно. Тиймээс өмнөх хос түлхүүрээ устгалгүй хадгалж байх шаардлага гардаг. Энэ шаардлагын дагуу түлхүүрийн түүхийг мэддэг, аль файлыг задлах, тайлахад аль түлхүүрийг ашиглахыг мэддэг байх ёстой. Гэхдээ шифрлэсэн файлаа тухай бүрд нь задлаад, өөр байдлаар шифрлэн хадгалсан бол хуучирсан хос түлхүүрийг заавал хадгалах шаардлагагүй, устгаж байж болно.

7) **Гэрчилгээнд хандах**: Хэд хэдэн хүлээн авагчид захидал, зурвас илгээх гэж буй хэрэглэгч тэдний гэрчилгээг хэрхэн олж авах вэ? НТДБ (Мон Пасс СА) эдгээр гэрчилгээг авах хялбархан татаж авах, үзэх тохиромжтой аргыг санал болгосон. Энэ зорилгоор Мон Пасс СА веб сан (repository) ажиллаж байна.

3.2 Тоон гарын үсгийн Үл Татгалзах Шинж

Тоон гарын үсгийн бас нэг чухал давуу тал нь түүнээс татгалзах боломжгүйд оршино. . Хэрэглэгч захиандаа, зурвасдаа тоон гарын үсэг зурсан бол түүнээс татгалзах боломжгүй болдог. Дэлхийд цорын ганц олгогдсон хосгүй хувийн түлхүүрээ ашиглан гарын үсэг зурж байгаа учир өөр хүн өмнөөс нь зурна гэсэн ойлголт байхгүй.

4. ДҮГНЭЛТ

НТДБ нь хурдтай хөгжиж буй өнөөгийн цахим орчинд ямар нэгэн эрсдэл аюулгүй системд нэвтрэх, захидал, зурвас, мэдээллээ баталгаажуулан илгээх, тэдгээрийг өөр хэн ч унших боломжгүйгээр шифрлэн илгээх боломжийг олгож байна. Итгэлтэй хөндлөнгийн тал болох ГОБ-ын сангаас шалгадаг, хувийн түлхүүр нь зөвхөн эзэмшигчид байдаг учир өгөгдлийн бүрэн бүтэн байдал, нууцлалыг бүрэн хангаж чаддаг.