FIGI
FINANCIAL INCLUSION
GLOBAL INITIATIVE

Аюулгүй байдал, дэд бүтэц, итгэлцлийн ажлын хэсэг

ДИЖИТАЛ САНХҮҮГИЙН ҮЙЛЧИЛГЭЭНИЙ АЮУЛГҮЙ БАЙДАЛ, БАТАЛГААЖУУЛАЛТЫН ХҮРЭЭ

АЮУЛГҮЙ БАЙДЛЫН АЖЛЫН ХЭСГИЙН ТАЙЛАН

ДИЖИТАЛ САНХҮҮГИЙН ҮЙЛЧИЛГЭЭНИЙ АЮУЛГҮЙ БАЙДАЛ, БАТАЛГААЖУУЛАЛТЫН ХҮРЭЭ

АНХААРУУЛГА

Санхүүгийн хүртээмжийн дэлхийн санаачилга (FIGI), Дэлхийн Банкны Групп (ДБГ), Төлбөр ба зах зээлийн дэд бүтцийн хороо (CPMI), Олон Улсын Цахилгаан Холбооны Холбоо (ITU) хамтран хэрэгжүүлдэг үндэсний санхүүгийн хүртээмжийн зорилтууд, дэлхийн 'Санхүүгийн бүх нийтийн хүртээмж 2020' зорилгод хүрэх зорилт бүхий 3 жилийн хөтөлбөр бөгөөд улс орны хэмжээнд шинэчлэлийг хэрэгжүүлэхэд дэмжлэг үзүүлэх зорилготой. Тус хөтөлбөр Билл & Мелинда Гейтсийн сан (BMGF)-ийн дэмжлэгтэй хэрэгждэг.

Хамтын ажиллагаа болон ерөнхий зохион байгуулалтын хувьд (1) Цахим төлбөр тооцоог нутагшуулах ажлын хэсэг (ДБАА удирдлагаар), (2) Дижитал санхүүгийн үйлчилгээн дэх танилт бүртгэл, хаяг ID -н ажлын хэсэг (ДБАА удирдлагаар), (3) Дэд бүтэц аюулгүй бадлыг бэхжүүлэх ажлын хэсэг (ОУЦХБ удирдлагаар) үүд ажиллаж тухайн улсын бодлого, зохицуулалтын байгууллага болон хувийн хэвшил, олон нийтийн санаа, санаачлагыг тусган уялдуулж хамтран ажиллаж байна.

Санхүүгийн хүртээмжийн дэлхийн санаачилга (FIGI)-ын хүрээнд үндэсний эрх баригчид хувийн хэвшил болон бусад холбогдох талуудыг оролцуулан тулгамдаж буй асуудал, шинээр гарч ирж буй ойлголтуудыг хуваалцах арга хэмжээг жил бүр 3 удаа зохион байгуулдаг.

Энэхүү тайлан нь Олон улсын цахилгаан холбооны байгууллагаар ахлуулсан аюулгүй байдал, дэд бүтэц, итгэлцлийн ажлын хэсгийн бүтээгдэхүүн юм. Энэхүү ажилд илэрхийлсэн дүгнэлт, тайлбар, дүгнэлтүүд нь Төлбөр ба зах зээлийн дэд бүтцийн хороо, Билл ба Мелинда Гейтсийн сан, Олон улсын цахилгаан холбооны байгууллага, Дэлхийн банк, Санхүүгийн хүртээмжийн дэлхийн санаачилгын түншүүдийн үзэл баримтлал биш бөгөөд шууд дагаж мөрдөх албагүй.

Тодорхой компаниуд эсвэл тодорхой үйлдвэрлэгчдийн бүтээгдэхүүнийг дурьдсан нь тэдгээрийг дурдаагүй бусад ижил төстэй шинж чанартай бүтээгдэхүүнээс илүүд зөвшөөрч, санал болгосон гэсэн үг биш юм. Алдаа, орхигдуулсан зүйлсийг эс тооцвол өмчийн бүтээгдэхүүний нэрсийг эхний том үсгээр ялгана. FIGI-ийн түншүүд энэ ажилд орсон мэдээллийн үнэн зөвийг баталгаажуулахгүй. Энэхүү бүтээлийн газрын зураг дээрх хил хязгаар, өнгө, нэр томъёо болон бусад мэдээлэл нь аливаа улс орон, нутаг дэвсгэр, хот, бүс нутгийн эрх зүйн байдлын талаарх FIGI-ийн түншүүдийн дүгнэлт, түүний эрх бүхий байгууллагуудын дүгнэлтийг илэрхийлэхгүй.

Энэ тайлангийн талаар

Энэхүү тайланг Флоридагийн их сургуулийн Кевин Батлер, ОУЦХБ-ын Вижай Мори нар бичсэн, Тайланг хянах, засварлахад дэмжлэг, туслалцаа үзүүлсэн Арнольд Кибуука, ОУЦХБ-д талархал илэрхийлье. Мөн санал шүүмжээ өгсөн Ассаф Клингер, Ваулто; Леон Перлман, Колумбын их сургууль; Рехан Масуд, Пакистаны Төрийн банк болон FIGI аюулгүй байдлын дэд бүтэц, итгэлцлийн ажлын хэсгийн гишүүдэд талархал илэрхийлье:.

Хэрэв та нэмэлт мэдээлэл өгөхийг хүсвэл Vijay Mauree-тэй tsbfigisit@itu.int хаягаар холбогдоно уу.

Агуулга

Хураангуй

Дижитал санхүүгийн үйлчилгээ (DFS) үзүүлэх нь банкууд, DFS үзүүлэгч, үүрэн холбооны операторууд (MNOs), DFS платформ нийлүүлэгчид, зохицуулагчид, агентууд, худалдаачид, төлбөрийн үйлчилгээ үзүүлэгчид, төхөөрөмж үйлдвэрлэгчид гэх мэт янз бүрийн оролцогч талуудын оролцоотой цогц экосистемийг хамардаг. Програм хөгжүүлэгчид, токен үйлчилгээ үзүүлэгчид, OEMs, үйлчлүүлэгчид. Эдгээр системийн байгууллагуудын харилцан уялдаа холбоо, экосистем дэх хэд хэдэн талуудад найдах нь ашуулгүй байдлын хил хязгаарыг дижитал санхүүгийн үйлчилгээ (DFS) үзүүлэгчээс гадна экосистем дэх үйлчлүүлэгчид, сүлжээний үйлчилгээ үзүүлэгчид, гар утас үйлдвэрлэгч болон бусад гуравдагч талын үйлчилгээ үзүүлэгчдэд хүргэдэг (тайлангийн 4.1 ба 4.2 ооc үзнэ үү).

Нэмж дурдахад, DFS үзүүлэгчид улам бүр төвөгтэй болж буй гар утасны экосистемтэй зохицон ажиллах нөхцөл тулгараад байна. Үйлдлийн систем бүрийн хувилбарт зориулсан аппликейшнүүдийг хөгжүүлэн эмзэг талуудыг тодруулах, арилгах зэргээр дэмжин ажиллаж байна. Энэхүү хурдацтай хөгжиж буй динамик орчинд DFS үзүүлэгчид ашуулгүй байдлын бодит ашуул заналхийллийн талаарх мэдлэг олгох, эрсдэлийг бууруулах, боломжит ашуул занлын хяналтын талаар тодорхой сорилтуудтай тулгардаг.

DFS Ашуулгүй байдлын баталгааны хүрээ нь DFS үзүүлэгчид (банкууд, цахим мөнгөний үйлчилгээ үзүүлдэг банк бусууд), үүрэн сүлжээний операторууд, үйлчлүүлэгчид, төлбөрийн системийн үйлчилгээ үзүүлэгчид, худалдаачид, технологийн үйлчилгээ/гуравдагч талын үйлчилгээнд тулгарч буй ашуулгүй байдал, эмзэг байдлын тоймыг өгхөд оршино.

Харилцаа холбооны салбарын зохицуулагчид, банк санхүү, төлбөрийн үйлчилгээний зохицуулагчид DFS-ний ашуулгүй байдлын суурь үзүүлэлтийг бий болгохын тулд тус ашуулгүй байдлын баталгааны хүрээг ашиглаж болно.

Энэхүү хүрээ нь хэрэгжсэнээр DFS экосистемд оролцож буй оролцогч талуудын тогтоосон эрсдэл, мэдээллийн ашуулгүй байдлын удирдлагын практикийг сайжруулах болно. Жишээлбэл, баримт бичигт байгаа ашуулгүй байдлын хяналтын арга хэмжээг DFS үзүүлэгчийн MXXT-ийн ашуулгүй байдлын хөтөлбөрийн нэг хэсэг болгон оруулж болно.

DFS Ашуулгүй байдлын баталгааны хүрээ нь дижитал санхүүгийн үйлчилгээг санал болгож буй талын хэрэгжүүлж болох ашуулгүй байдлын эрсдлийг удирдах зохион байгуулах аргачлалыг санал болгож байна:

- Дижитал санхүүгийн үйлчилгээнд үйлчлүүлэгчдийн итгэх итгэлийг нэмэгдүүлнэ.
- Экосистем дэх оролцогч талуудын үүрэг, хариуцлагыг тодорхой болгох.
- Экосистем дэх ашуулгүй байдлын эмзэг цэг болон ашуул заналыг тодорхойлох.
- Эцсийн цэг хүртэл ашуулгүй байдлын хяналтыг бий болгох.
- DFS-ийн бүх оролцогч талуудыг хамарсан ашуулгүй байдлын эрсдлийн удирдлагын менежментийн туршлагыг бэхжүүлэх.

DFS Ашуулгүй байдлын баталгааны хүрээ нь ашуул занал, эмзэг байдлыг үнэлэх ашуулгүй байдлын эрсдлийн удирдлагын системтэй үйл явцыг хангаж, хэрэглэгч, хөдөлгөөнт төхөөрөмж, үүрэн холбооны оператор болон DFS үйлчилгээ үзүүлэгчид чиглэсэн ашуул заналхийллийн үед DFS үйлчилгээ үзүүлэгч болон үүрэн холбооны операторoос хэрэгжүүлэх ашуулгүй байдлын хяналтын зохих арга хэмжээг тодорхойлдог.

Худалдаачид, төлбөрийн үйлчилгээ үзүүлэгч болон бусад санхүүгийн үйлчилгээний байгууллагуудтай холбоотой ашуул заналхийлэл, түүнийг засах, арилгах тусгай арга хэмжээ нь энэ баримт бичигт хамаарахгүй.

Энэхүү тайлан нь Кибер ашуулгүй байдлын ажлын хүрээнд Ашуулгүй байдал, дэд бүтэц, итгэлцлийн ажлын хэсэг дэх санхүүгийн үйлчилгээний байгууллагуудад кибер ашуулгүй байдлын нөхцөл байдлыг удирдах, хариу арга хэмжээ авах аргачлалын талаар хийсэн ажлын үр дүн юм.

DFS ашуулгүй байдлын баталгааны хүрээ нь дараах бүрэлдэхүүн хэсгүүдээс бүрдэнэ.

a) ISO/IEC 27005 – Ашуулгүй байдлын арга техник - Мэдээллийн ашуулгүй байдлын эрсдлийн менежмент (тайлангийн 7-р хэсэг) дээр суурилсан ашуулгүй байдлын эрсдэлийн удирдлагын арга зүй.
b) Үүрэн холбооны оператор болон DFS үйлчилгээ үзүүлэгч, DFS програмууд, үйлчилгээнүүд, сүлжээний үйл ажиллагаа болон DFS хүргэх экосистемд оролцож буй гуравдагч талын үйлчилгээ үзүүлэгчдийн суурь дэд бүтцэд учирч буй ашуул занал, эмзэг байдлын үнэлгээ.
c) Дээрх (b)-ын үр дүнд тулгуурласан нөлөөллийг бууруулах стратеги. Тайлангийн 8-р хэсэгт дурдсан ашуулгүй байдал болон хяналтыг бууруулах арга хэмжээг тодорхойлсон.

Тайлангийн 9-р хэсэгт DFS үйлчилгээ үзүүлэгчдийн апп-ын ашуулгүй байдлын бодлогын баримт бичигт оруулж болох ашуулгүй байдлын шилдэг туршлагын загварыг өгсөн болно. Үүнд програмын нарийн үзүүлэлтүүдийг тусгасан бөгөөд зөвлөмжийг тайлбарласан дэд хэсгүүд нь үйл ажиллагааны янз бүрийн асуудлуудыг тусд нь тодорхойлсон. Гар утасны үйлдлийн системд олон зөвлөмжийг ашиглах боломжтой хэдий ч зах зээлд эзлэх хувь хэмжээнд үндсэлэн Android програмууд дээр төвлөрсөн. Тайлангийн 10-р хэсэгт DFS-тэй холбоотой ашуулгүй байдал, ослыг удирдах хүрээг тусгасан болно.

Тайлан байнга засагдаж сайжирч байх амьд баримт бичиг байх зорилготой бөгөөд шинэ платформ, хэрэглээ, үйлчилгээ, цаг хугацааны явцад үүсэх ашуул, шинэ эмзэг байдлыг цаг тухайд нь шинэчлэн тусгах юм.

Товчлол

API	Application Programming Interface	Хэрэглээний програмчлалын интерфейс
DFS	Digital Financial Services	Дижитал санхүүгийн үйлчилгээ
GW	Gateway	Гарц
HCE	Hosted Card Emulation	Хост картын эмуляц
HLR	Home Location Register	Гэрийн байршлын бүртгэл
HSM	Hardware Security Module	Техник хангамжийн аюулгүй байдлын модуль
IMEI	International Mobile Equipment Identity	Олон улсын хөдөлгөөнт төхөөрөмжийн таних тэмдэг
IMSI	International Mobile Subscriber Identity	Олон улсын гар утасны захиалагчийн таних тэмдэг
ISO	International Organization for Standardization	Олон улсын стандартчиллын байгууллага
ITU	International Telecommunication Union	Олон улсын цахилгаан холбооны байгууллага
ITU FGDFS	ITU Focus Group on Digital Financial Services	ОУЦХБ-ын дижитал санхүүгийн үйлчилгээний төвлөрсөн бүлэг
IVR	Interactive Voice Response	Интерактив дуут хариу(автомат хариулагч)
MFA	Multi-Factor Authentication	Олон хүчин зүйлийн баталгаажуулалт
MNO	Mobile Network Operator	Үүрэн холбооны оператор
MSC	Mobile Switching Centre	Үүрэн холбооны холболтын байгууламж
MSISDN	Mobile Station International Subscriber Directory Number	Мобайл станцын олон улсын захиалагчийн лавлах дугаар
MST	Magnetic Secure Transmission	Хамгаалалттай соронзон дамжуулалт'Samsung pay'
MVNO	Mobile Virtual Network Operator	Үүрэн холбооны виртуал оператор
NFC	Near Field Communication	Ойрын зайн холбоо
OS	Operating System	Үйлдлийн систем
OTP	One Time Password	Нэг удаагийн нууц үг
OWASP	Open Web Application Security Project	Вэб програмын аюулгүй байдлын нээлттэй төсөл
PA-DSS	Payment Application Data Security Standard	Төлбөрийн хэрэглээний мэдээллийн аюулгүй байдлын стандарт
PCI-DSS	Payment Card Industry Data Security Standard	Төлбөрийн картын мэдээллийнаюулгүй байдлын тандарт
POS	Pont of Sale	төлбөр авах цэг ПОС
PSD2	Payment Services Directive 2	Төлбөрийн үйлчилгээний заавар 2
QR Code	Quick Response Code	Шуурхай хариу өгөх код
RP	Relying Party	Онлайн нөөцөд хандах хүсэлтийг боловсруулдаг сервер
SCA	Strong Customer Authentication	Хүчэтгэсэн хэрэглэгчийн баталгаажуулалт
SD	Security Dimension	Хамгаалалтын хэмжүүр үзүүлэлт
SE	Secure Element - A formally certified, tamper-resistant, stand-alone integrated circuit often referred to as a “chip” as defined by the European Payments Council or other recognized standards authority.	Хамгаалалтын элемент - Европын Төлбөрийн Зөвлөл эсвэл бусад хүлээн зөвшөөрөгдсөн стандартын эрх бүхий байгууллагаас тодорхойлсон албан ёсоор баталгаажуулсан, хөндлөнгийн оролцоонд тэсвэртэй, бие даасан нэгдсэн хэлхээг, ихэвчлэн "чип" гэж нэрлэдэг.
SIM	Subscriber Identity Module	Захиалагчийг таних модуль
SMS	Short Messaging Service	Богино т эмдэгтмессежийн үйлчилгээ
STK	SIM Toolkit	SIM хэрэгслийн багц
TEE	Trusted Execution Environment	баталгаажсан гүйцэтгэлийн орчин
TPP	Third-Party (Payment Service) Providers	Гуравдагч этгээдийн (төлбөрийн үйлчилгээ) нийлүүлэгчид
TSP	Token Service Provider	Токен үйлчилгээ үзүүлэгч
UICC	Universal Integrated Circuit Card	Universal Integrated Circuit Card
URL	Uniform Resource Locator	Нөөцийн нэгдмэл байршуулагч
USSD	Unstructured Supplementary Service Data	Бүтэцгүй нэмэлт үйлчилгээний өгөгдөл

Дижитал санхүүгийн үйлчилгээний аюулгүй байдал, баталгаажуулалтын хүрээ

1. ТАНИЛЦУУЛГА

Дижитал технологи нь ашиглахад хялбар, боломжийн үнэтэй, өргөжүүлэх, хөгжүүлэх боломжтой, тав тухтай, харилцагч төвтэй байдлаар санхүүгийн үйлчилгээг сая сая хүмүүст хүргэж санхүүгийн хүртээмжтэй болоход түлхэц өгсөн.

Дэлхийн банкны Global Findex мэдээллийн сангаас [1] *“Дэлхий даяарх насанд хүрсэн иргэдийн дижитал төлбөр тооцоо хийх буюу хүлээн авах хувь хэмжээ 2014-2017 оны хооронд 11 пунктээр өссөн байна. Өндөр орлоготой эдийн засагтай орнуудад насанд хүрэгчдийн 51 хувь нь (данс эзэмшигчдийн 55 хувь) сүүлийн нэг жилд дор хаяж нэг санхүүгийн гүйлгээг цахимаар хийсэн гэж мэдээлсэн. гар утас эсвэл интернет ашиглах. Хөгжиж буй эдийн засагтай орнуудын насанд хүрэгчдийн 19 хувь (данс эзэмшигчдийн 30 хувь) нь гар утасны данс, гар утас эсвэл интернет ашиглан дор хаяж нэг шууд төлбөр хийсэн гэж мэдээлсэн* .

Гэсэн хэдий ч үйлчилгээ үзүүлэгчид илүү өргөн хүрээний санхүүгийн үйлчилгээг санал болгох дижитал хэрэгслийг цуглуулж, илүү үр дүнтэй, үйл ажиллагааны зардал багатай байгаа тул дижитал санхүүгийн үйлчилгээний хурдацтай өсөлт, хэрэглээ нь түүний экосистемийг аюулгүй байдлын янз бүрийн аюул заналхийлэлд өртөмтгий болгож байна.

Системийн байгууллагуудын харилцан уялдаа холбоо, экосистем дэх хэд хэдэн талуудын оролцоо нь дижитал санхүүгийн үйлчилгээ (DFS) үзүүлэгчээс гадна хэрэглэгчид, сүлжээний үйлчилгээ үзүүлэгчид, гар утас үйлдвэрлэгчид болон бусад гуравдагч талын үйлчилгээ үзүүлэгчдийн аюулгүй байдлын хил хязгаарыг хамаатуулан өргөжүүлдэг.

Нэмж дурдахад, DFS үзүүлэгчид улам бүр төвөгтэй болж буй гар утасны экосистемтэй ажиллах ёстой бөгөөд үйлдлийн системийн олон хувилбарт зориулсан аппликейшнүүдийг тус бүр өөрийн гэсэн эмзэг талтай хөгжүүлж, өөр өөр төрлийн хөдөлгөөнт төхөөрөмжүүдийг дэмждэг. Энэхүү хурдацтай хөгжиж буй динамик орчинд DFS үйлчилгээ үзүүлэгчид аюулгүй байдлын бодит аюул заналхийллийн талаарх мэдлэг, эрсдэлийг бууруулах боломжтой аюулгүй байдлын хяналтын талаар тодорхой сорилтуудтай тулгарсаар байна.

DFS Аюулгүй байдлын баталгааны хүрээ нь дээрх мэдлэгийн зөрүүг нөхөх зорилготой бөгөөд дижитал санхүүгийн үйлчилгээний (DFS) экосистемийн оролцогч талууд дараах зорилгоор хэрэгжүүлж болох аюулгүй байдлын эрсдлийг удирдах зохион байгуулалтын аргачлалыг санал болгож байна.

- Дижитал санхүүгийн үйлчилгээнд үйлчлүүлэгчдийн итгэх, итгэлийг нэмэгдүүлнэ.
- Экосистем дэх оролцогч талууд түс бүрийн үүрэг, хариуцлагыг тодорхой болгох.
- Экосистем дэх аюулгүй байдлын эмзэг тал болон холбогдох аюул, заналхийлэлийг тодорхойлох.
- Төгсгөлийн аюулгүй байдлыг хангахын тулд аюулгүй байдлын хяналтыг бий болгох.
- DFS-ийн бүх оролцогч талуудыг хамарсан аюулгүй байдлын эрсдэлийн удирдлагын менежментийн туршлагыг бэхжүүлэх.

DFS Аюулгүй байдлын баталгааны хүрээ нь DFS үйлчилгээ үзүүлэгчид (банкууд, цахим мөнгөний үйлчилгээ үзүүлдэг банк бусууд), үүрэн сүлжээний операторууд, үйлчлүүлэгчид, төлбөрийн системийн үйлчилгээ үзүүлэгчид, худалдаачид, технологийн үйлчилгээ/гуравдагч талын үйлчилгээнд тулгарч буй аюул, занал эмзэг байдлын тоймыг өгдөг.

Харилцаа холбооны зохицуулагч, бодлого тодорхойлогчид, банк санхүү, төлбөрийн зохицуулагчид зэрэг зохицуулагчид мөн DFS үйлчилгээ үзүүлэгчдийн аюулгүй байдлын суурь үзүүлэлтийг бий болгоход ашиглаж болно.

Уг хүрээ нь DFS экосистемд оролцож буй талуудын тогтоосон эрсдэл, мэдээллийн аюулгүй байдлын удирдлагын практикт дэмжлэг үзүүлэх болно. Жишээлбэл, баримт бичигт туссан “аюулгүй байдлын хяналтын арга хэмжээг” DFS үйлчилгээ үзүүлэгчийн МХХТ-ийн аюулгүй байдлын хөтөлбөрийн нэг хэсэг болгон оруулж болно.

Байгууллагууд мэдээллийн аюулгүй байдлын бодлогын баримт бичиг, өгөгдлийн ангилал, мэдээллийн аюулгүй байдлын үүрэг хариуцлагын хуваарилалт, мэдээллийн нууцлалын бодлого, ажилтнуудаа аюулгүй байдлын мэдлэг, сургалт, аюулгүй хөгжүүлэлт, туршилт, засвар үйлчилгээ зэрэг аюулгүй байдлын сайн засаглалын зарчим, стандартуудыг аль хэдийн хэрэгжүүлсэн гэсэн үндсэн таамаглалыг дэвшүүлж байна. дэд бүтэц, төхөөрөмж, программууд болон процессууд, эмзэг байдлын менежмент, нөөцлөх журам, ослын менежмент, бизнесийн тасралтгүй байдал, гамшгаас хамгаалах үйл явц

Аюулгүй байдлын баталгааны хүрээ нь ITU-T зөвлөмж X.805-ыг сүлжээний төгсгөлийн аюулгүй байдалд хүрэхийн тулд аюулгүй байдлын хяналтын арга хэмжээг хэрэгжүүлэх үндэс болгон ашигладаг бөгөөд мөн "Дижитал санхүүгийн аюулгүй байдлын асуудлууд" техникийн тайланд гарсан зөвлөмжид үндэслэн хяналтыг голчлон санал болгодог. Үйлчилгээ” [2.] ITU-T Focus group Digital Financial Services.

2. ITU-T ЗӨВЛӨМЖ X805 ТОЙМ

DFS экосистемийн эцсийн хэрэглэгч хүртлэх харилцаа холбооны орчныг ITU-T-ийн зөвлөмж X.805-ийн үүднээс авч үзсэн бөгөөд аюулгүй байдлын менежментэд хэрэгтэй лавлагааны хүрээг бүрдүүлдэг. ITU-T зөвлөмжийн X.805 аюулгүй байдлын архитектур нь сүлжээний аюулгүй байдлын тодорхой асуудлыг шийдвэрлэхэд зориулагдсан найман" *аюулгүй байдлын хэмжүүр "-тэй.*

Сүлжээний аюул заналтай тулгарах системчилсэн арга замыг хангадаг аюулгүй байдлын найман хэмжигдэхүүн нь дараах байдалтай байна.

- **Хандалтын хяналт:** Сүлжээний нөөцийг зөвшөөрөлгүй ашиглахаас хамгаалах.
- **Баталгаажуулалт:** Харилцагч байгууллагуудын хувийн мэдээллийг баталгаажуулах аргууд.
- **Үл татгалзах:** Хувь хүн эсвэл аж ахуйн нэгж аливаа үйл явдал, үйлдлийн шалтгааныг үгүйсгэхээс сэргийлэх арга.
- **Мэдээллийн нууцлал:** Мэдээлэл задруулахаас хамгаалах.
- **Харилцаа холбооны аюулгүй байдал:** Мэдээллийг өөр тийш нь шилжүүлэх, хөндлөнгөөс оролцохгүйгээр зөвхөн зөвшөөрөгдсөн цэгүүдийн хооронд дамжуулдаг гэдгийг баталгаажуулах.
- **Өгөгдлийн бүрэн бүтэн байдал:** Өгөгдлийн үнэн зөв, бодит байдлыг хамгаалах.
- **Бэлэн байдал:** Сүлжээний элементүүд болон өгөгдөлд зөвшөөрөл олгохыг хориглохоос урьдчилан сэргийлэх.
- **Нууцлал:** Сүлжээний үйл ажиллагааг ажигласнаар өгөгдлийн мэдээллийг хамгаалах.

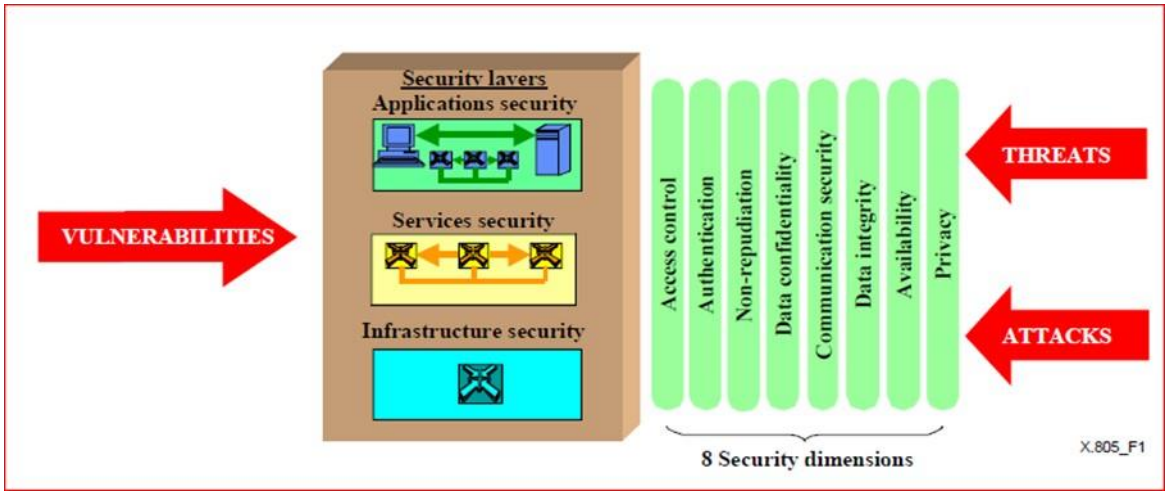
ITU-T зөвлөмж X.805 нь сүлжээний тоног төхөөрөмж болон байгууламжийн бүлгүүдийн шатлалыг аюулгүй байдлын гурван давхарга болгон тодорхойлсон. Эдгээр аюулгүй байдлын давхаргууд нь аюулгүй байдлын цогц шийдлээр хангадаг бөгөөд давхарга бүр өөр өөр төрлийн аюул заналхийлэл, халдлагад өртөж болзошгүй тул бүтээгдэхүүн, шийдлүүдийн аюулгүй байдлын талаар хаана анхаарах ёстойг тодорхойлдог. Аюулгүй байдлын давхаргууд нь дараах байдалтай байна.

i. **Дэд бүтцийн аюулгүй байдлын давхарга:** харилцаа холбооны сүлжээ, үйлчилгээ, хэрэглээг бий болгоход ашигладаг үндсэн барилгын блокуудаас бүрдэх ба бие даасан дамжуулах холбоосууд, тэдгээрийн үндсэн техник хангамж, програм хангамжийн платформ зэрэг сүлжээний элементүүдээс бүрдэнэ.

ii. **Үйлчилгээний аюулгүй байдлын давхарга:** хэрэглэгчид/эцсийн хэрэглэгчдийн сүлжээнээс хүлээн авдаг үйлчилгээнүүдээс бүрдэнэ. Эдгээр үйлчилгээ нь үндсэн холболт, тээвэрлэлтээс хамаарна

iii. **Аппликэйшнүүдийн аюулгүй байдлын давхарга:** хэрэглэгчид/эцсийн хэрэглэгчдийн ханддаг сүлжээнд суурилсан програмууд дээр төвлөрдөг.

Зураг 1 - ITU-T зөвлөмж X.805 Хамгаалалтын үзүүлэлтүүд



3. DFS-ний БИЗНЕСИЙН ЗАГВАРУУД

DFS экосистемийн долоон гол оролцогчыг авч үздэг: DFS хэрэглэгч, худалдаачин, төрийн болон төрийн бус байгууллага, Үүрэн холбооны оператор (MNO), банк, гуравдагч этгээд, Үүрэн холбооны виртуал сүлжээ бүхий оператор (MVNO). Мөн бид эдгээр оролцогч талуудын хувьд хадгаламж эзэмшигч, цахим мөнгө гаргагч, төлбөрийн үйлчилгээ үзүүлэгч, агент сүлжээний менежер, үүрэн холбооны үйлчилгээ үзүүлэгч гэсэн таван үндсэн чиг үүргийг авч үздэг.

Оролцогч талуудын гүйцэтгэсэн үүргээс хамааран бид DFS үйлчилгээ үзүүлэгчийн хамгийн түгээмэл дөрвөн бизнесийн загварыг авч үздэг.

a) Банк удирдсан

b) MNO удирдсан

c) MVNO

d) Гибрид

3.1 Банк удирдсан бизнесийн загвар

Энэ загварт банкнаас санал болгож буй санхүүгийн үйлчилгээг гар утасны хэрэглэгчдэд хүргэдэг бөгөөд бүртгүүлэх үйл явц нь банк эсвэл агентийн сүлжээгээр дамждаг. Энэ загварт банк санхүүгийн гол үүргийг гүйцэтгэдэг, өөрөөр хэлбэл хадгаламж эзэмшигч, цахим мөнгө гаргагч, төлбөрийн үйлчилгээ үзүүлэгч юм. Эдгээр санхүүгийн үйлчилгээг хэрэглэгчдэд хүргэх харилцаа холбооны сүлжээг Бүтцгүй нэмэлт үйлчилгээний өгөгдөл (USSD), богино мессежийн үйлчилгээ (SMS), интерактив дуут хариу (IVR) гэх мэт өөр өөр сувгуудаар дамжуулан MNO хангадаг. SIM програмын хэрэгсэл (STK). Жишээлбэл, Бангладеш дахь United Commercial банкнаас санал болгож буй Ucash Доорх 2-р зураг банктай загварын дүрслэлийг үзүүлэв

Зураг 2 - Банкаар удирдуулсан бизнесийн загвар

3.2 MNO удирдсан бизнесийн загвар

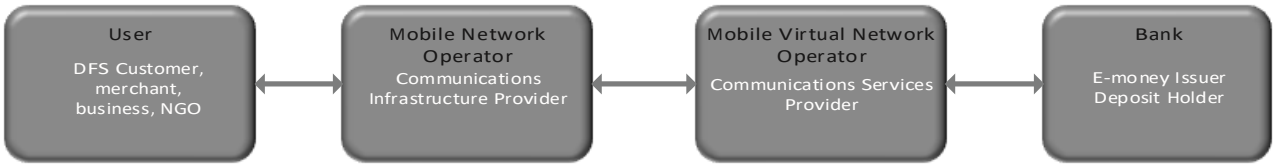
MNO удирдсан загварт харилцаа холбооны сүлжээг хангах уламжлалт үүргийн зэрэгцээ MNO нь санхүүгийн үүргийн дийлэнх хэсгийг хариуцдаг бөгөөд ингэснээр цахим мөнгө гаргах, агентийн сүлжээ, харилцагчийн харилцааг удирдах бөгөөд төлбөрийн үйлчилгээ юм. үйлчилгээ үзүүлэгч. MNO нь DFS-ийн хэрэглэгчдийг бүртгэж, тэднээс цахим мөнгөний оронд MYOX-ны нэрийн өмнөөс бодит бэлэн мөнгө авдаг DFS агентийн өргөн сүлжээг удирддаг. Санхүүгийн горимоос хамааран МУБХ нь түнш банктай хамтран ажиллахыг шаардаж болох бөгөөд DFS-ийн агентууд МНБ-ын нэрийн өмнөөс харилцагчдаас цуглуулсан мөнгөн хөрөнгийг байршуулах болно. MNO-аас гаргасан цахим мөнгө нь түнш банкин дахь итгэлцлийн буюу эскроу дансанд байгаа мөнгөөр баталгааждаг бөгөөд жишээ нь Safaricom-ын M-PESA, Airtel Money, MTN Mobile Money юм.

Зураг 3 - MNO led business model

3.3. Үүрэн холбооны виртуал сүлжээ бүхий операторгой загвар

Зарим хэрэгжүүлэлтүүдэд DFS-д шаардлагатай харилцаа холбооны үйлчилгээг үзүүлдэг Mobile Virtual Network Operator (MVNO) байдаг. MVNO нь бие даасан эсвэл банкны эзэмшилд байж болно. Жишээ нь, Кени улсын Equity Bank, Equitel, MVNO-г эзэмшдэг бөгөөд банкны санхүүгийн үйлчилгээг гар утасны сүлжээний хэрэглэгчиддээ цахим мөнгө хэлбэрээр хүргэдэг. MVNO-ууд нь MNO-ийн хангасан дэд бүтцийг ашигладаг боловч хэрэглэгчиддээ дижитал санхүүгийн үйлчилгээ зэрэг харилцаа холбооны өөр төрлийн үйлчилгээг санал болгоно. MNO болох Airtel нь Equitel-ийн утасгүй сүлжээний дэд бүтцийг хангадаг.

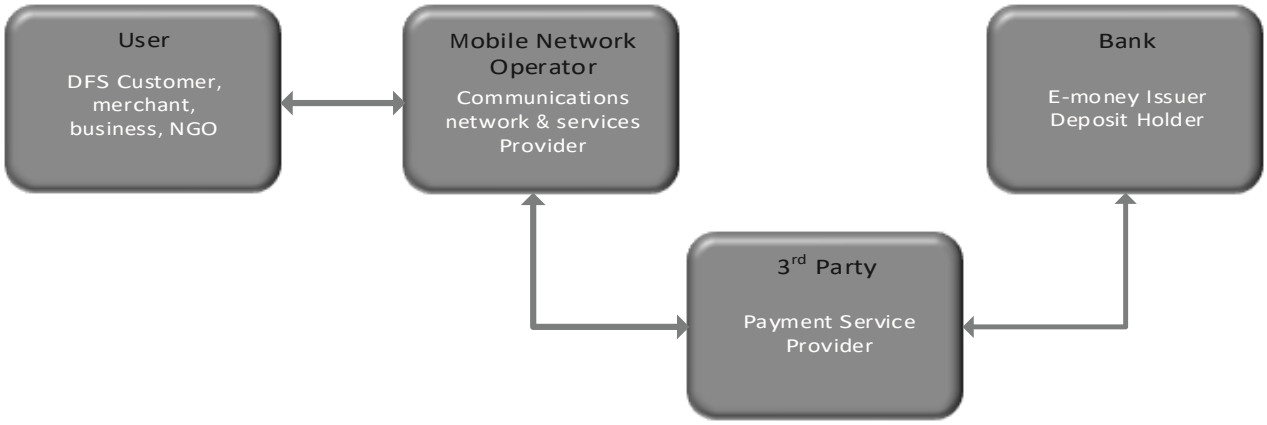
Зураг 4 - MVNO загвар



3.4. Гибрид загвар

Гибрид загварт чухал үүргийг банк болон MNO хооронд хуваадаг. Тэд экосистемийн гуравдагч этгээдийг татан оролцуулж болох бөгөөд энэ нь МҮБ болон банкнаас үзүүлдэггүй үйлчилгээ үзүүлдэг. Жишээлбэл, гуравдагч этгээд төлөөлөгчийн сүлжээг эзэмшиж болох бөгөөд төлбөрийн үйлчилгээ үзүүлэгчийн үүргийг гүйцэтгэдэг. Жишээлбэл, Visa Qiwi түрийвч

Зураг 5 - Гибрид загвар



4. DFS ЭКОСИСТЕМИЙН ЭЛЕМЕНТҮҮД

Энэхүү тайлангийн хүрээнд гар утасны төлбөрийн таван ангиллыг багтаасан болно.

- Үйлчлүүлэгчийн гар утасны төхөөрөмж (жишээ нь MPESA) дээр татаж авсан төлбөрийн тусгай програмгүйгээр МҮБХ-ны сувгууд (жишээ нь SMS, USSD, дуут утас) ашиглан гар цахим мөнгө шилжүүлэх.
- Банкны данс, дебит карт эсвэл кредит карттай холбогдсон хэрэглэгчийн гар утасны төхөөрөмж дээрх гар утасны төлбөрийн програм (жишээ нь Square, Venmo, Facebook messenger)
- Холбоо барихгүйгээр төлбөрийн технологи: Харилцаа холбоогүй төлбөрийн технологи нь хэрэглэгчийн гар утасны төхөөрөмжөөс худалдааны POS руу төлбөрийн өгөгдлийг илгээхэд янз бүрийн төрлийн харилцаа холбооны технологийг ашиглах боломжтой дижитал түрийвчийг ашиглах явдал юм. Мэдээллийг POS руу дамжуулахад ашигладаг зарим харилцаа холбооны технологид Near Field Communication (NFC), QR код, соронзон хамгаалалттай дамжуулалт (MST), Bluetooth, SMS, интернет орно. Дижитал түрийвчийг хэрэглэгчийн гар утасны төхөөрөмж эсвэл үүлэн дээр хадгалах боломжтой.
- Near Sound Data Transfer (NSDT) Төлбөр: NSDT нь төлбөрийн гүйлгээний өгөгдлийг шифрлэхийн тулд гар утасны аудио сувгийг ашигладаг.
- Алсын төлбөр: Үүнд Интернэт төлбөр (цахим худалдааны вэб сайт дээрх зээлийн картаар/карт дээрх гүйлгээ), оператор компанийн шууд тооцоо, SMS хураамжийн төлбөр, мобайл банк орно.

Дижитал валютын түрийвч (жишээ нь Bitcoin) энэ тайлангийн хамрах хүрээнээс гадуур байна.

Дараагийн хэсгүүдэд DFS экосистемийн элементүүдийг авч үзэх болно:

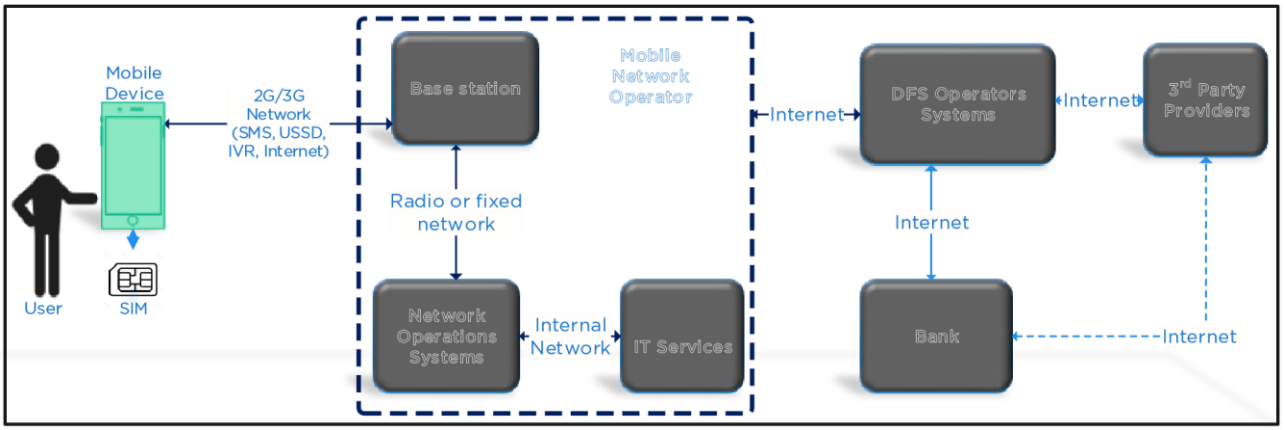
1) USSD, SMS, IVR болон STK ашиглан гар утасны төлбөр хийх 2) Цахим төлбөрийн хэрэглүүр болон дижитал түрийвч (жишээлбэл, Google Pay, Apple Pay, WeChat Pay).

USSD, SMS, IVR, STK болон NSDT ашиглан DFS экосистемийн 41 элемент

Зураг 6-д экосистемийн үндсэн бүрэлдэхүүн хэсгүүдийг харуулав. Элемент бүрийг байршуулалт бүрт ашиглахгүй; жишээлбэл, DFS үйлчилгээнд ашиглах боломжтой Wi-Fi хандалт эсвэл ухаалаг утасны програм байхгүй тохиолдолд хэрэглэгчийн харилцаа холбоо нь интернетийн гадаад гарцаар эсвэл үүлэн үйлчилгээнд найдах гэхээсээ илүү гар утасны сүлжээгээр дамжих харилцаанд хязгаарлагдана.

Экосистемийн бүх оролцогч талууд нь дараахь зүйлсээс бүрдэнэ.

Зураг 6 - DFS экосистемийн үндсэн элементүүд



a) **Хэрэглэгч/Хэрэглэгч:** Үйлчлүүлэгч нь DFS үйлчилгээний зорилтот үзэгчид бөгөөд үйлчилгээтэй харилцахын тулд цахим мөнгөний програмыг ашигладаг. Ийм харилцан үйлчлэл нь шууд, Үүрэн холбооны сүлжээгээр эсвэл интернетээр дамжуулан (үндсэн гар утасны платформ болон цахим мөнгөний програмын онцлогоос хамаарч) явагдах боломжтой; Өөрөөр хэлбэл, харилцагчийн нэрийн өмнөөс DFS үйлчилгээтэй харилцдаг DFS агент ийм харилцан үйлчлэлийг зуучилж болно. Агент нь сүлжээнд шууд холбогдох эсвэл ийм үйлчилгээ үзүүлэхийн тулд вэб гарцыг ашиглах боломжтой.

b) **Мобайл төхөөрөмж:** Хөдөлгөөнт төхөөрөмж нь цахим мөнгөний програмыг ашиглах платформоор хангадаг. Энэ нь үйлчлүүлэгч (эсвэл үйлчлүүлэгчийн нэрийн өмнөөс харилцдаг агент; тайлбарлахад хялбар байх үүднээс агентаас тусгайлан шаардах арга хэмжээ аваагүй л бол үйлчилгээтэй хийх цаашдын бүх харилцан үйлчлэл нь үйлчлүүлэгчээр

дамждаг гэж үздэг) гол суваг юм. DFS үйлчилгээ. Хөдөлгөөнт төхөөрөмжүүд нь гар утас эсвэл ухаалаг гар утас байж болно. Хязгаарлагдмал нөөцийг агуулсан, хэрэглээний хязгаарлагдмал интерфэйсийг дэмждэг, мөн хязгаарлагдмал холболтын сонголттой (жишээ нь, 2G GSM үйлчилгээ) онцлог утаснууд. Нөгөө талаас ухаалаг гар утаснууд нь аюулгүй техник хангамжийн элементүүд болон дэвшилтэт сүлжээ, Wi-Fi холболтыг дэмждэг маш хүчирхэг үйлчилгээг дэмждэг. Утас болон ухаалаг гар утас хоёулаа SIM карттай бөгөөд тэдгээрийн зарим нь аппликешнээр ашиглах боломжтой хамгаалалтын элементүүдийг агуулдаг. Хөдөлгөөнт төхөөрөмж нь үйлдлийн системтэй бөгөөд түүний чадвар нь түүнд байгаа нөөцөөс хамаарна. Symbian OS-ийн загварчилсан хөнгөн үйлдлийн системүүд нь ихэвчлэн онцлог утсанд байдаг бол ухаалаг гар утсанд ихэвчлэн Android, IOS, Windows болон бусад үйлдлийн системийг суулгасан байдаг.

c) **Суурь станц:** Суурь станц болон гар утасны хоорондох холбоо нь хэрэглэгч болон DFS үйлчилгээ үзүүлэгчийн хооронд мэдээлэл дамжуулах үндсэн суваг юм. Аппликейшнүүдийг гар утсанд хүргэдэггүй, харин оронд нь нээлттэй сүлжээг ашигладаг системүүдэд (жишээ нь SMS, STK, IVR болон USSD-д суурилсан харилцаа холбоо) энэ холбоос нь дамжуулагдсан өгөгдөлд шифрлэлт хийгдсэн ерөнхий архитектурын цорын ганц хэсэг юм. Хэрэглэгч рүү болон хэрэглэгчээс – үндсэн станцад өгөгдөл хүлээн авмагц үйлчилгээ үзүүлэгчийн сүлжээгээр шифрлэгдээгүй илгээгдэнэ. Энэ холбоос нь бат бөх, найдвартай, хаа сайгүй түгээмэл байх нь DFS системийн тогтвортой байдал, боломжийн хувьд амин чухал юм.

d) **Үүрэн холбооны сүлжээ:** Операторын сүлжээ нь хэрэглэгчийн гар утаснаас мэдээлэл дамжуулах боломжийг олгодог. Энэ нь гадаад үйлчилгээ үзүүлэгч болон DFS үйлчилгээ үзүүлэгчтэй холбогдох өөр өөр гарцууд, тухайлбал тухайн тээвэрлэгчтэй холбоотой эсвэл интернет холболт шаарддаг гадны байгууллага байж болох өөр өөр гарцуудыг багтаасан харилцаа холбоог идэвхжүүлдэг өөр өөр зангилаанаас бүрдэнэ. Энэ сүлжээнд USSD, IVR, STK, SMS гэх мэт гарцууд, HLR, VLR гэх мэт дотоод мэдээллийн сан, DFS үйлчилгээ үзүүлэгчтэй холбогдох боломжтой интернет гарцууд байрладаг. Үүрэн холбооны сүлжээний оператор нь DFS үйлчилгээ үзүүлдэг тохиолдолд тэдгээр үйлчилгээнд нэвтрэх гарц нь тэдний дотоод сүлжээнд хадгалагдана. Хөдөлгөөнт шилжих төв (MSC) нь HLR эсвэл VLR-ийн хэрэглэгчийн өгөгдлийг ашиглан харилцаа холбоог чиглүүлэхэд хялбар болгохын тулд гар утасны сүлжээн дэх өөр өөр зангилааны гол цөм юм. Хавсралт 1-д Үүрэн холбооны сүлжээний нарийвчилсан сүлжээний зангилаа, SMSC gateway (GW), SAT(SIM Application Toolkit) GW, USSD gateway, IVR болон интернет GW нь хэрэглэгчдэд холбогдох хандалтын горимуудыг ашиглах боломжийг олгодог, бид мөн MNO-г харуулав. SMS, IVR эсвэл интернетийн төлбөрт зориулж MNO зарим байршуулалтад ашигладаг төлбөрийн систем. Үүрэн холбооны виртуал сүлжээ бүхий оператор (MVNO) нь DFS үйлчилгээ үзүүлэгч болон хэрэглэгчдэд MNO-ийн үйлчилгээг үзүүлж болох боловч утасгүй сүлжээний дэд бүтцийг сүлжээний оператор эсвэл идэвхжүүлэгч хангасан хэвээр байна.

e) **DFS үйлчилгээ үзүүлэгч:** DFS үйлчилгээ үзүүлэгч нь мобайл үйлдлийн системээс гаралтай програмын агуулгыг холбодог.

Санхүүгийн үйлчилгээ үзүүлэгчидтэй сүлжээ байгуулж, үйлчлүүлэгчийн мэдээллийг аюулгүйгээр удирдаж, аудит зэрэг үйлчилгээ үзүүлэх боломжийг олгодог. Эдгээр үйлдлүүдийг аюулгүй байлгахын тулд DFS оператор нь өгөгдөлд нэвтэрч бүй хүн нь өөрсдийгөө хэн мөн гэдэгт итгэлтэй байх ёстой. Сүлжээний өгөгдлийн агуулгыг үнэлэх, DFS програмаар дамжуулан өгсөн тушаалуудыг үнэлэхийн тулд аудитын бүртгэлийг идэвхжүүлсэн байх ёстой. Хэрэглэгчийн хэн болохыг тодорхойлох, баталгаа (эрх) олгох, хэрэглэгчийн гүйлгээний өгөгдлийг хадгалах, гуравдагч этгээдэд зориулсан API гэх мэт интерфейсийг идэвхжүүлэх, янз бүрийн эх сурвалжаас гүйлгээг боловсруулах зэрэг нь DFS операторын гүйцэтгэдэг үүрэг юм.

f) **Гуравдагч этгээдийн үйлчилгээ үзүүлэгчид:** Гадны үйлчилгээ үзүүлэгчид нь үүрэн холбооны операторт суурилсан цахим мөнгөний системүүдийн хооронд харилцан үйлчлэлцэх боломжийг олгож, банкны дэд бүтэц гэх мэт арын санхүүгийн сүлжээнүүдтэй холбогдох үндэс суурийг бүрдүүлдэг. Эдгээр гадны үйлчилгээ үзүүлэгчдийн гүйцэтгэж болох бусад үүрэгт мэдээллийн технологийн системийг ажиллуулах эсвэл хэрэглэгчийн дэмжлэг үзүүлэх зэрэг багтдаг бөгөөд зарим тохиолдолд тэдгээр нь DFS системүүдийн хооронд шууд холбогдох эсвэл үйлчилгээ, гүйлгээний нэгтгэгчийн үүрэг гүйцэтгэдэг.

g) **Санхүүгийн дижитал үйлчилгээний програм:** Энэхүү програм нь үйлчлүүлэгч DFS экосистемтэй харилцах интерфейсийг хангадаг. Аппликейшн нь USSD, STK эсвэл SMS-ээр харилцах зориулалттай тусгай утсан дээрх цэсэнд суурилсан системээс эхлээд IVR ашигладаг дуут дизайн эсвэл ухаалаг гар утсан дээрх баялаг график интерфэйс хүртэл интерфэйсүүд болон үйлчлүүлэгчдэд өгдөг туршлагаараа ихээхэн ялгаатай байж болно. Интернэт стандартын криптограф алгоритмаар хангагдсан тээврийн хэрэгслийн төгсгөлийн аюулгүй байдал. Код, нууц үг, хурууны хээ гэх мэтээр идэвхжүүлсэн програмын тусгай цэсийг ашиглан харилцан үйлчлэл үүсч, хэрэглэгчдэд мөнгө илгээх, төлбөр тооцоо хийх, эфирийн цаг цэнэглэх, дансны үлдэгдлийг шалгах боломжтой.

Програм болон дижитал түрийвч дээр суурилсан DFS экосистемийн 42 элемент (жишээ нь Google Pay, Apple pay, WeChat Pay, Samsung Pay)

Дижитал түрийвчний загварт суурилсан экосистемд өөр өөр элементүүд байдаг бөгөөд гол загваруудын дунд; төхөөрөмж төвтэй гар утасны хэтэвч, төхөөрөмж төвтэй гар утасны апп доторх түрийвч, карт байхгүй картон файл түрийвч, QR код болон дижитал тооцооны түрийвч. Эдгээр нь бүгд өөр өөр технологийн платформтой бөгөөд аюулгүй байдлын өөр өөр загваруудыг ашигладаг.

Бид энэ экосистемийн бүрэлдэхүүн хэсэг бүрийг доор тайлбарлав.

а) хөдөлгөөнт төхөөрөмж

Хөдөлгөөнт төхөөрөмж нь гар утасны түрийвч рүү нэвтрэх платформоор хангадаг бөгөөд энэ нь дижитал түрийвч/аппликейшн, төхөөрөмжийн үйлдлийн систем болон DFS болон програмын өгөгдлийг хамгаалах түлхүүр хамгаалалтын элементийг агуулдаг.

Доорх зураг нь хэрэглэгчийн гар утасны төхөөрөмжийн зарим бүрэлдэхүүн хэсгүүдийг харуулж байна.

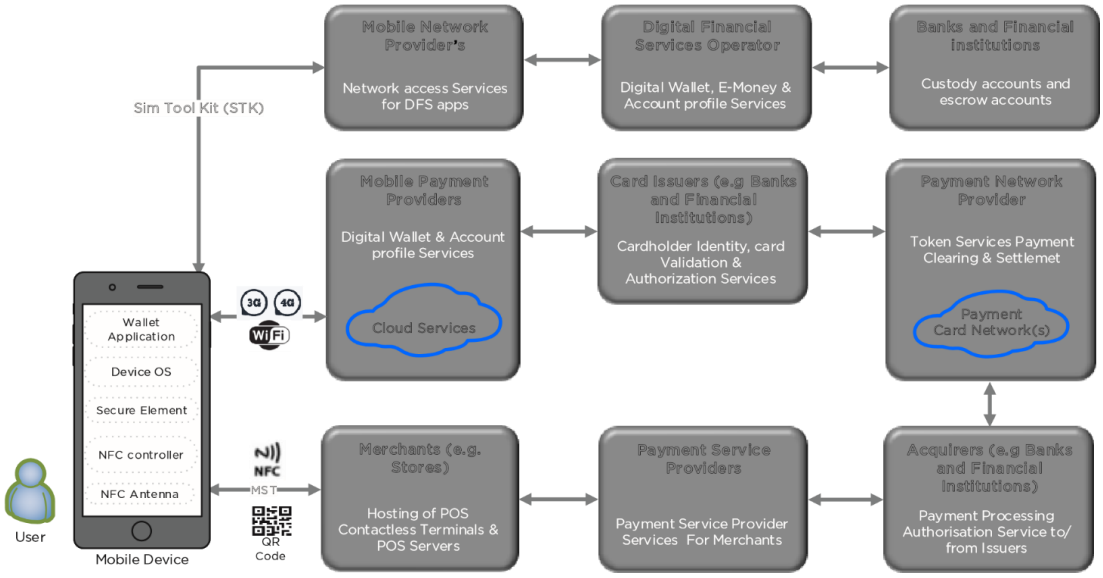
i. **NFC хянагч ба NFC антен:** NFC хянагч нь Ойролцоох талбарын холбооны протоколуудыг зохицуулж, программ ба Secure Element болон Secure Element болон борлуулалтын цэгийн терминал хоорондын холболтыг чиглүүлдэг. NFC антен нь хянагч болон ПОС терминалын хоорондох дохиог дамжуулдаг.

ii. **Secure Element:** Secure Element (SE) нь хөндлөнгийн нөлөөнд тэсвэртэй платформ бөгөөд ихэвчлэн программууд болон тэдгээрийн нууц болон криптограф өгөгдлийг найдвартай байршуулахад зориулагдсан нэг чипийн хамгаалалттай микроконтроллер юм. SE-ийн хэрэглээ нь гар утасны түрийвчний хэрэглээний төрөл, гар утасны төлбөрийн горимын төрлөөс хамаарна, жишээлбэл, Apple-ийн төхөөрөмжүүдийн SE нь Apple Pay-д ашиглах үед картыг дуурайдаг. Төрөл бүрийн төлбөрийн хэрэглүүрүүд эсвэл дижитал түрийвчний шаардлага, тэдгээрийн зах зээлийн хэрэгцээг хангах зорилгоор SE нь өөр өөр хэлбэрээр байдаг. SE нь iPhone дээрх SE гэх мэт хөдөлгөөнт төхөөрөмжийн техник хангамжид суулгагдсан, нэгтгэгдсэн байж болно. SE нь SIM/UICC байж болно, GSM стандартыг ашигладаг сүлжээнүүд үүнийг илүү түгээмэл SIM Toolkit (STK) програмууд хэлбэрээр илүүд үздэг бөгөөд SIM картыг аюулгүй цахим мөнгөний хэрэглүүрийг санал болгох аюулгүй элемент болгон ашигладаг. SE нь хөдөлгөөнт төхөөрөмжид залгах боломжтой аюулгүй санах ойн карт байж болно.

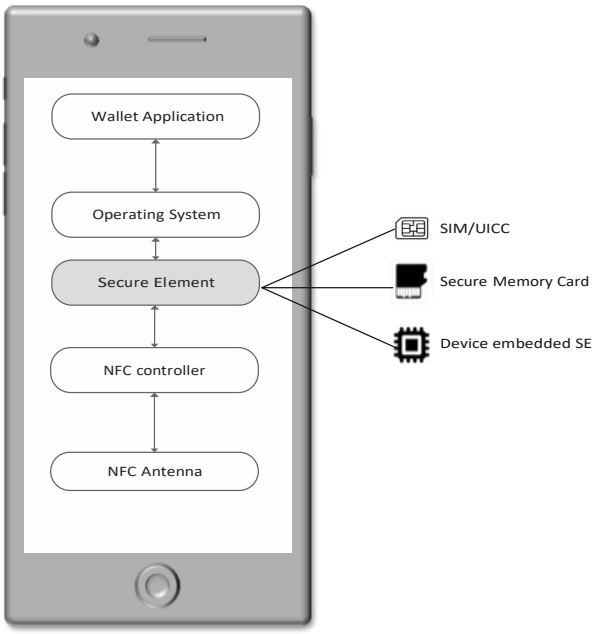
iii. **Хост картын эмуляци:** Хөдөлгөөнт төхөөрөмжүүд нь төлбөрийн картын өгөгдөл гэх мэт эмзэг өгөгдлийг хадгалахад техник хангамжийн аюулгүй байдлын элементэд тулгуурладаггүй Хост картын эмуляцийг (HCE) ашиглан контактгүй картыг дуурайж чаддаг. HCE нь гар утасны түрийвчний аппликейшн нь NFC хянагчаар дамжуулан найдвартай харилцах боломжийг олгодог програм хангамжийн дэд бүтцийн шийдэл юм. . HCE нь Google Pay-г дэмжихийн тулд Android гар утасны төхөөрөмжүүдэд ихэвчлэн ашиглагддаг.

Доорх Зураг 7 нь програмууд болон дижитал түрийвч дээр суурилсан экосистемийг харуулж байна.

Зураг 7 - Програмууд болон дижитал түрийвч дээр суурилсан DFS экосистем



iv. **Цахим түрийвч:** цахим түрийвч нь төхөөрөмжөөр дамжуулан ханддаг програмууд /үйлчилгээнүүд бөгөөд Зураг 8,-Хөдөлгөөнт төхөөрөмжийн бүрэлдэхүүн хэсгүүдийг зөвшөөрдөг түрийвч эзэмшигч нь төлбөр гэх мэт санхүүгийн гүйлгээнд найдвартай нэвтрэх, удирдах, гүйцэтгэх. Samsung Pay, Apple Pay зэрэг гар утасны түрийвч нь тухайн төхөөрөмж болон программ хангамжид зориулагдсан бөгөөд зээлийн болон дебит картыг орлуулах боломжтой. Нөгөөтэйгүүр, бусад гар утасны/дижитал түрийвч нь төхөөрөмжийн үл хамаарах шинж чанартай бөгөөд хэрэглэгчийн төлбөрийн мэдээлэл, нууц үгийг олон тооны төлбөрийн хэрэгсэл, вэб сайтад найдвартай хадгалдаг бөгөөд энэ нь гүйлгээг хялбар, хурдан гүйцэтгэх боломжийг олгодог бөгөөд биометр, бусад дижитал түрийвчний жишээ гэх мэт илүү хүчтэй баталгаажуулалтыг ашиглах боломжийг олгодог. Эдгээр нь Google Pay, WeChat pay, Paypal, Alipay юм.



б) худалдаачин

Худалдаачид үйлчлүүлэгчдээс бараа, үйлчилгээний төлбөрийг борлуулалтын цэгийн терминал эсвэл QR кодыг сканнердах эсвэл төлбөрийн хэрэглүүрт худалдагчийн дугаар оруулах зэрэг бусад хэрэгслээр хүлээн авдаг. Мобайл төхөөрөмжийг худалдаачид төлбөр хийхдээ ашигладаг бөгөөд энэ нь эмзэг байдлын өөр нэг эх үүсвэр юм.

в) Борлуулалтын цэгийн терминалууд

Борлуулалтын цэг (POS) терминал нь худалдаачны байршилд гар утасны төлбөр тооцоог боловсруулахад ашигладаг цахим төхөөрөмж юм. ПОС терминал ба мобайл төхөөрөмжийн хоорондох төлбөр тооцооны сувгууд, контактгүй. NFC, QR код эсвэл Соронзон зурвас (MST) ашигладаг. 3G, 4G, Wi-Fi сүлжээг гар утасны хэтэвчэнд өргөн ашигладаг. Компьютер эсвэл зөөврийн компьютер дээр байгаа аливаа эрсдэл хөдөлгөөнт төхөөрөмж дээр ч байж болно.

Суурин компьютер болон зөөврийн компьютеруудын стандарт харилцааны аргуудын зэрэгцээ хөдөлгөөнт төхөөрөмжүүд нь үүрэн холбооны олон технологи (жишээ нь, LTE болон GSM), GPS, Bluetooth, хэт улаан туяа (IR), NFC чадамжийг агуулж болно. Зөөврийн (жишээ нь, SIM карт болон SD карт) технологийн туршилтанд ашигладаг дотоод электрон төхөөрөмж, суулгагдсан мэдрэгч, биометрийн уншигч зэрэг эрсдэлийг нэмэгдүүлнэ.

i. **Near Field Communication (NFC):** NFC нь радио давтамжийн технологид суурилсан утасгүй холбооны протокол бөгөөд хоорондоо хэдхэн см зайтай төхөөрөмжүүдийн хооронд мэдээлэл солилцох боломжийг олгодог. NFC идэвхжүүлсэн гар утасны төхөөрөмж дээрх түрийвч нь төлбөр тооцоог удирдаж, эхлүүлдэг гар утсанд хадгалагдсан програм хангамжийн програм юм. Хөдөлгөөнт түрийвч нь баталгаажсан орчинд төлбөрийн карт, банкны данс, үнэнч үйлчилгээний купон эсвэл гар утсанд хадгалагдсан санхүүгийн мэдээлэл зэрэг төлбөрийн баталгаанд ханддаг. Зайлшгүй холболттой ПОС терминалын ойролцоо гар утсыг товших буюу барих замаар төлбөрийн гүйлгээг эхлүүлэхэд физик харилцааг ашигладаг.

ii. **Magnetic Strip Technology (MST):** Magnetic Secure Transmission буюу MST нь уламжлалт төлбөрийн карт шиг соронзон дохио үүсгэдэг. Дараа нь соронзон дохиог төхөөрөмжөөс ПОС терминал руу илгээдэг. MST зарим Samsung гар утсан дээр идэвхжсэн.

iii. **QR кодууд:** QR кодууд нь контактгүй төлбөрийн хувилбаруудыг хоёр аргаар санал болгодог.

a. Төлбөр төлөгч нь худалдаачны QR кодыг уншдаг, худалдаачин гүйлгээний QR код үүсгэдэг эсвэл өөрт ногдсон статик QR кодыг харуулах ба төлбөр төлөгч нь утасныхаа камер ашиглан кодыг сканнердах ба төлбөрийн хэрэглүүр нь гүйлгээг эхлүүлэхийн тулд төлбөр эсвэл худалдааны дэлгэрэнгүй мэдээллийг оруулдаг. ПИН кодоо оруулснаар гүйлгээ хийгддэг.

b. Худалдаачин төлбөр төлөгчийн QR кодыг уншдаг; үйлчлүүлэгч төлбөрийн хэрэгслээр дамжуулан худалдаачинд гүйлгээний өвөрмөц QR код үүсгэх болно; худалдаачин QR сканнер ашиглан төлбөрийн хэрэгслээр дамжуулан кодыг сканнердаж, ПИН код оруулснаар гүйлгээг эхлүүлнэ.

iv. **3G/4G болон WiFi**

3G болон 4G үүрэн сүлжээнээс гадна хөдөлгөөнт төхөөрөмжүүд нь утасгүй (Wi-Fi) сүлжээнд холбогдох боломжтой бөгөөд эдгээр сүлжээ нь төхөөрөмж дээрх гар утасны програмыг төлбөрийн үйлчилгээ үзүүлэгчтэй харилцах боломжийг олгодог. 3G, 4G, WiFi сүлжээг ихэвчлэн Үүрэн холбооны оператор хангадаг.

d. **Токен үйлчилгээ үзүүлэгч (TSP)**

TSP нь жетонуудын амьдралын мөчлөгийг удирддаг. Нэмэлт үйлчилгээнд гол төлөв токен үүсгэх, хадгалах, токенуудын амьдралын мөчлөгийг удирдах, жетон гүйлгээг боловсруулах, токеноос PAN-д зураглал хийх, карт эзэмшигчийн баталгаажуулалт, үүнд нөөцийн үйлчилгээ, HCE ашиглан төхөөрөмжид суурилсан түрийвчний түлхүүрийн удирдлага, гүйлгээний баталгаажуулалтын үйлчилгээ орно. төхөөрөмжийн хүчинтэй байдал.

e. **Худалдан авагч**

Худалдаачны гүйлгээг холбогдох үнэт цаас гаргагч банкуудад дамжуулж төлбөр хүлээн авах санхүүгийн байгууллага эсвэл банкийг хүлээн авагч гэнэ.

f. **Үнэт цаас гаргагч**

Үнэт цаас гаргагч нь картын сүлжээ, үйлчилгээг төлөөлөн хэрэглэгчдэд зээлийн карт гаргадаг санхүүгийн байгууллага юм

g. **Түрийвчний үйлчилгээ үзүүлэгч (WSP)**

WSP нь гар утасны төлбөрт төрөл бүрийн харилцаа холбооны технологийг ашигладаг тусгайлсан түрийвчний шийдлүүдийг санал болгодог.

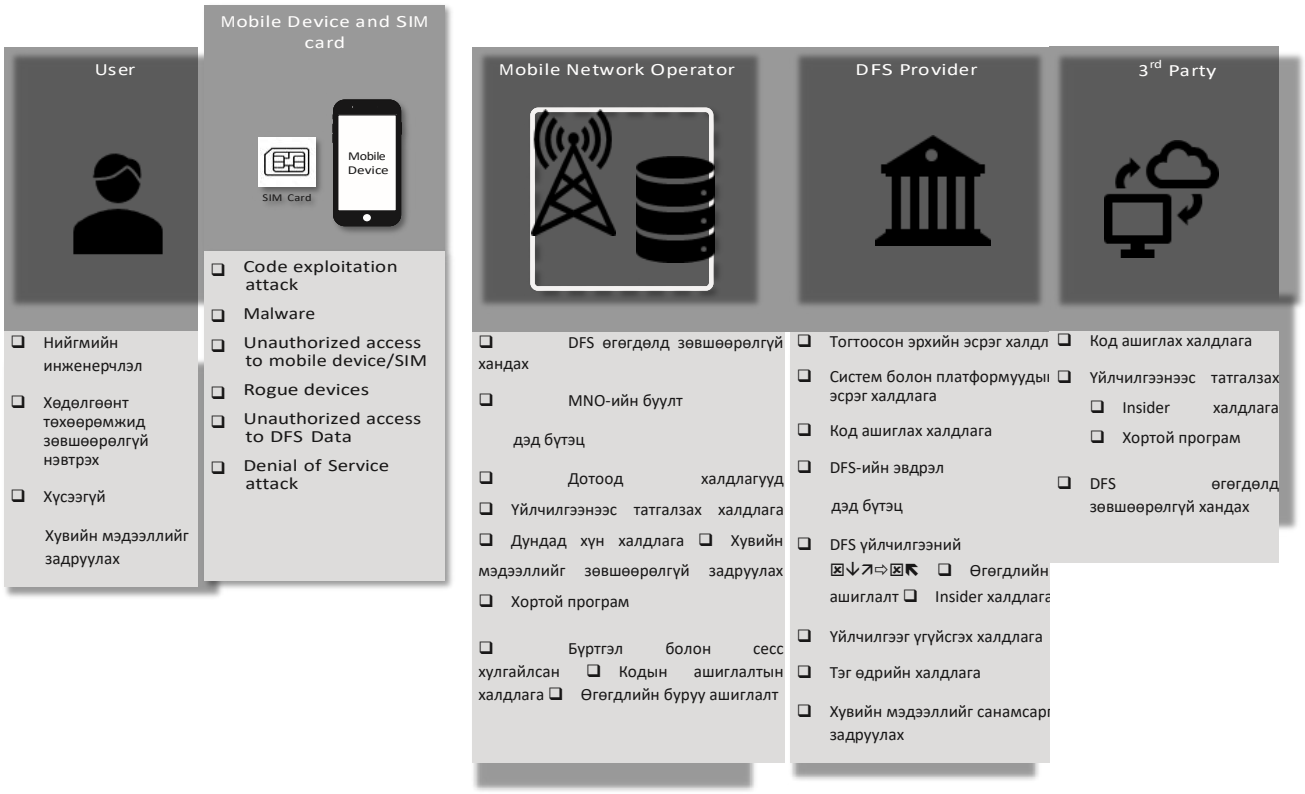
h. **Төлбөрийн үйлчилгээ үзүүлэгч (PSP)**

PSP нь худалдаачинд гар утас болон дижитал түрийвчнээс төлбөр хүлээн авах боломжийг олгодог янз бүрийн аргуудыг өгдөг. PSP нь олон хүлээн авагчид болон төлбөрийн болон картын сүлжээнд холбогдох боломжтой. PSP үйлчилгээнд хамрагдсанаар PSP нь банкны данс, гадаад сүлжээтэй харилцах харилцааг удирдах боломжтой тул гүйлгээг удирдахад санхүүгийн байгууллагуудаас хамаарал багасна.

5. АЮУЛГҮЙ БАЙДАЛ, АЮУЛ ЗАНАЛ

5.1. USSD, SMS, IVR, STK болон NSDT ашиглан DFS -д учирч болох аюулууд Доорх диаграммд USSD, SMS, IVR, STK болон NSDT дээр суурилсан DFS програмуудын аюулыг нэгтгэн харуулав.

Зураг 9 - USSD, SMS, IVR болон NSDT ашиглан DFS системд учирч буй аюулууд



5.2. Аппликейшн болон дижитал түрийвч дээр суурилсан DFS экосистемд учирч болох аюул занал

Цахим төлбөрийн хэрэглүүр/түрийвч нь ес дээр суулгасан программуудаар дамжуулан зөвхөн Samsung төхөөрөмж болон Apple-ийн санхүүгийн үйлчилгээнд дижитал төлбөр төлөх боломжийг олгодог бол Google Pay-г бүх андроид мобайл төхөөрөмж, санхүүгийн хэрэглүүрийн шинж чанар, Quick tion болон бусад үйлчилгээ бүхий гар утасны төлбөрийн хэрэглүүр дээр ашиглах боломжтой. Ашигласан сувгууд нь төхөөрөмжөөс хамаарна WeChat Pay болон AliPay зэрэг хариу өгөх кодууд нь чадамж байж болно, жишээ нь Samsung pay болон Apple-ийн камер бүхий бүх ухаалаг гар утсанд ашиглагддаг.

Хүснэгт 1 – Програмууд болон дижитал түрийвч дээр суурилсан DFS экосистемд учирч болох аюулын хураангуй

Элемент	Аюул заналхийлэл
Цахим төлбөрийн програм	• Хэрэглээний эх кодын урвуу инженерчлэл • Цахим төлбөрийн аппликейшнд хөндлөнгөөс оролцох • Цахим төлбөрийн програмын сул талыг ашиглах • Хортой програм суулгах • Мобайл үйлдлийн системд нэвтрэх зөвшөөрөл, авах
Гар утас	• Хуурамч програмууд болон хортой програмуудыг суулгах • Алдагдсан эсвэл хулгайлагдсан хөдөлгөөнт төхөөрөмжид зөвшөөрөлгүй нэвтрэх • Төхөөрөмж дээр хортой програм суулгах

Худалдаачдын заналхийлэл	• OS-ийн хортой програм: Халдагчид алсаас хандах болон төлбөрийн өгөгдөлд ашиглаж болох POS төхөөрөмж дээр POS хортой программыг байршуулж болзошгүй. • QR кодын эвдрэл: QR кодууд нь хүний нүдээр амархан уншигдах боломжгүй тул аюул заналхийлэлтэй байдаг тул халдагчид худалдаачдын QR кодыг хортой контент агуулсан хор хөнөөлтэй кодоор амархан сольж болно. Хортой контент нь фишинг URL, хортой гар утасны програм байж болно. • POS-н контактгүй терминал болон ПОС серверийн эсрэг халдлага: Халдагчид худалдаачдын дотоод сүлжээг хамгаалахын тулд галт хана байхгүй гэх мэт сүлжээний аюулгүй байдлын сул талыг ашиглаж болно. • NFC идэвхжүүлсэн ПОС-ын контактгүй терминалуудын эсрэг релей халдлага: Хөдөлгөөнт төхөөрөмж дээр суулгасан реле программ хангамж нь утасгүй сүлжээгээр гар утасны POS дээр прокси болгон суулгасан Secure Element болон карт эмуляторын хооронд тушаал, хариу дамжуулах боломжтой. • POS терминалуудад хандахын тулд өгөгдмөл ПИН-г ашиглах, жишээлбэл, өгөгдмөл 166816 болон Z66816 (1)
Худалдан авагчид	• Төлбөрийн боловсруулалтын систем эвдэрч байна: Гаргагчийн төлбөрийн сүлжээнээс жетон болон криптограммыг хүсэх үед халдагчид дотоод сүлжээний төлбөр боловсруулах серверүүдийн аль нэгэнд хортой программ хангамж болон алсаас хандах хэрэгслийг суулгаснаар карт эзэмшигчийн их хэмжээний мэдээллийг олж авах боломжтой. • Сүлжээний болон интерфейсийн аюулгүй байдлыг алдагдуулж, халдагчид сүлжээний үйлчилгээ үзүүлэгчийг эвдэх замаар хүлээн авагч болон гаргагчийн хоорондох найдвартай бус холболтыг ашиглаж болно, халдагчид API дуудлагыг хянах, удирдах боломжтой болохын тулд энэ түвшний хандалтыг ашиглах боломжтой.
Төлбөрийн үйлчилгээ үзүүлэгч	• Төлбөрийн гарцын эвдрэл: Худалдаачдаас хүлээн авагч банк руу дамжих гүйлгээний өгөгдөлд нэвтрэх, халдах зорилгоор төлбөрийн гарцыг халдагчид онилж болно. • Карт байгаа, контактгүй төлбөр тооцоо, карт байхгүй гэх мэт өөр өөр сувгуудын өгөгдлийг боловсруулах боломжтой PSP-ээс худалдаачдад олгодог POS-ийн контактгүй терминалуудын програм хангамжийн эмзэг байдлын эвдрэл. • Аюулгүй сүлжээнүүдийн эвдрэл; Халдагчид нь PSP-ээс хүлээн авагч руу дамжуулж буй нууц мэдээллийг хууран мэхлэхийн тулд Man in the middle халдлага хийж болно. Үйлчилгээ үзүүлэгч нь TLS болон SSL-ийн доод хувилбарууд зэрэг сул эсвэл найдвартай холболтуудыг ашиглаж байгаа тохиолдолд. • ПОС терминалын машинууд болон ПОС системүүд болон хүлээн авагчид хүрэх/төлбөрийн гарцууд дахь алдаа, засваргүй програм хангамжийн эмзэг байдлыг төлөвлөх.
Үнэт цаас гаргагчид	• Төлбөрийн боловсруулалтын систем эвдэрч байна: Гаргагчийн төлбөрийн сүлжээнээс жетон болон криптограммыг хүсэх үед халдагчид дотоод сүлжээний төлбөр боловсруулах серверүүдийн аль нэгэнд хортой программ хангамж болон алсаас хандах хэрэгслийг суулгаснаар карт эзэмшигчийн их хэмжээний мэдээллийг олж авах боломжтой. • Сүлжээний болон интерфейсийн аюулгүй байдлыг алдагдуулж, халдагчид сүлжээний үйлчилгээ үзүүлэгчийг эвдэх замаар хүлээн авагч болон гаргагчийн хоорондох найдвартай бус холболтыг ашиглаж болно, халдагчид API дуудлагыг хянах, удирдах боломжтой болохын тулд энэ түвшний хандалтыг ашиглаж болно.

Төхөөрөмж/аппликейшн болон төлбөрийн үйлчилгээ үзүүлэгчийн хоорондох дижитал төлбөрийн хэрэглүүрүүдийн харилцаа нь Wi-Fi, 3G, 4G сүлжээгээр дамжуулан интернет сувагт тулгуурладаг. Соронзон аюулгүй дамжуулалт, сканнер ашиглан худалдааны цэгийн борлуулалтын төхөөрөмжид төлбөр хийх боломжтой. Түргэн хариу өгөх код эсвэл NFC зэрэг орно.

Эдгээр сувгийг ашиглах нь бусад аюул заналхийлэл, элементүүдийг (ПОС, хүлээн авагч, төлбөрийн сүлжээний үйлчилгээ үзүүлэгч, карт гаргагч, гар утасны төлбөрийн үйлчилгээ үзүүлэгч) харуулдаг.

Эдгээр бүрэлдэхүүн хэсгүүдэд үндэслэн бид мобайл аппликейшн болон түрийвч (жишээ нь Android, iOS) дээр суурилсан DFS экосистемд учирч болох дараах аюулуудыг тодорхойлдог.

DFS экосистемийн оролцогч талуудад үндэслэн бид худалдаачид, худалдан авагчид, төлбөрийн үйлчилгээ үзүүлэгч болон үнэт цаас гаргагчдыг гуравдагч талын үйлчилгээ үзүүлэгч гэж үздэг (бид эдгээр бие даасан аж ахуйн нэгжүүдийг **Хавсралт 1 дэх DFS экосистемийн өргөтгөсөн зураг харуулав**).

Бид эдгээр байгууллагад тулгарч буй ерөнхий аюулыг энд жагсааж байгаа хэдий ч тэдэнд тулгарч буй аюул заналыг арилгах тусгай арга хэмжээ нь энэ баримт бичигт хамаарахгүй.

Бид PCI-DSS-тэй зөвлөлдөхийг зөвлөж байна. DFS аюулгүй байдлын баталгааны хүрээ нь ISO/IEC 27000 мэдээллийн аюулгүй байдлын удирдлагын систем, төлбөрийн картын үйлдвэрлэлийн мэдээллийн аюулгүй байдлын стандарт (PCI-DSS) v3.2, төлбөрийн хэрэглээний мэдээллийн аюулгүй байдлын стандарт (PA) -ын ижил төстэй зарчмуудыг баримталдаг. -DSS), Үндэсний Стандарт, Технологийн Хүрээлэнгийн Тусгай хэвлэл 800-53, зэрэгт тусгагдсан.

6. DFS АЮУЛГҮЙ БАЙДЛЫН БАТАЛГААНЫ ХҮРЭЭ

Аюулгүй байдлын төвийн техникийн удирдамж (CIS controls Version 7), OWASP шилдэг 10 гэж нэрлэдэг Нээлттэй вэбийн аюулгүй байдлын хэрэглээний төсөл (OWASP) мөн эдгээрийг дижитал санхүүгийн үйлчилгээний экосистемд хамаарах хяналтыг тодорхойлоход жишиг болгон ашигласан.

Энэхүү хүрээ нь дараахь бүрэлдэхүүн хэсгүүдээс бүрдэнэ.

a) ISO/IEC 27005 – Аюулгүй байдлын техник – Мэдээллийн аюулгүй байдлын эрсдлийн удирдлага (**7-р хэсэг**) стандартад суурилсан аюулгүй байдлын эрсдлийн үнэлгээ.

b) Суурь дэд бүтэц, DFS програм, үйлчилгээ, сүлжээний үйл ажиллагаа болон DFS хүргэх экосистемд оролцож буй гуравдагч талын үйлчилгээ үзүүлэгчдийн аюул, эмзэг байдлын үнэлгээ (**8-р хэсэг**).

c) (b)-ын үр дүнд тулгуурласан нөлөөллийг бууруулах стратеги

дээрх (**8-р хэсэг**). Энэ хүрээ нь тодорхойлдог

i. Аюулгүй байдлын хэмжигдэхүүн тус бүр дэх DFS хөрөнгийн янз бүрийн аюулгүй байдлын аюул занал

ii. Эдгээр аюул заналхийллээр ашиглаж болох холбоотой сул талууд.

iii. DFS-ийн оролцогч талууд аюул занал, эмзэг байдлын эсрэг хэрэгжүүлж болох аюулгүй байдлын хяналтын арга хэмжээг санал болгож байна. Аюулгүй байдлын хяналтын хэмжүүр нь ITU-T X.805 зөвлөмжийн аюулгүй байдлын найман хэмжигдэхүүний нэг буюу хэд хэдэн хэсэгт багтаж болно.

7. ЭРСДЛИЙН ҮНЭЛГЭЭНИЙ АРГАЧЛАЛ

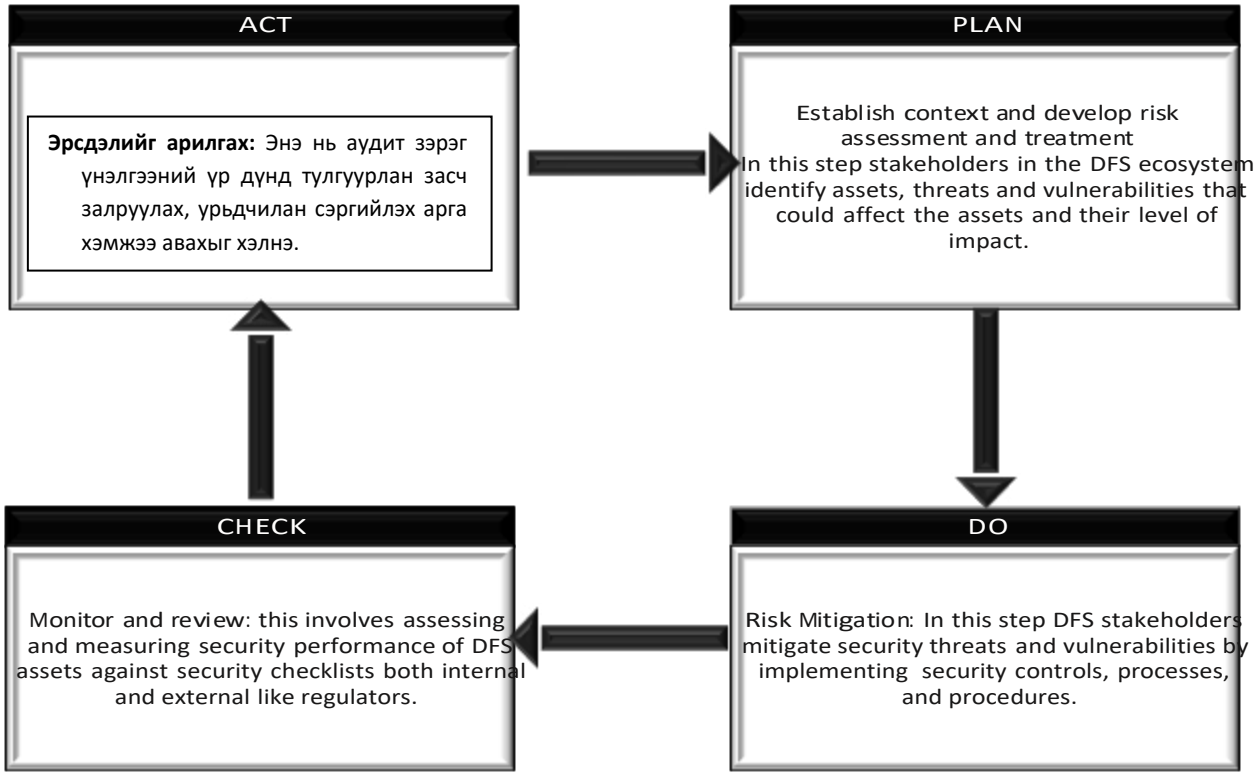
Тогтвортой, DFS-ийн аюулгүй байдлыг тасралтгүй сайжруулдаг аюулгүй байдлын загварыг хангахын тулд энэхүү хүрээ нь Төлөвлөх, гүйцэтгэх, Шалгах, Үйлдлэх (PDCA) гэсэн дөрвөн үе шатанд хуваагдсан дөрвөн үе шаттай чанарын загвар болох Демингийн циклийг ашигладаг. PDCA-д суурилсан хэрэгжүүлэх арга зүйд дөрвөн үе шат бүрт хүрэх ёстой үйл ажиллагаа, үр дүнг тус бүр тодорхойлсон.

DFS экосистемд олон оролцогч талууд оролцдог бөгөөд PDCA нь DFS экосистемийн төгсгөлөөс төгсгөл хүртэл аюулгүй байдлыг хангах үйл ажиллагаануудаас бүрдэх бөгөөд доорх диаграммд PDCA дээр суурилсан DFS аюулгүй байдлын хүрээний загварыг харуулав.

DFS орчны хяналт-шинжилгээ нь оролцогч талуудаас хамааран өөр өөр хэлбэртэй байж болно, жишээлбэл, зохицуулагч нь DFS хэрэглэгчдийн аюулгүй байдлыг хангахын тулд DFS үйлчилгээ үзүүлэгчээс тогтоосон аюулгүй байдлын хяналтыг хянадаг эсвэл аудиторууд DFS орчны дотоод болон гадаад үнэлгээг хийдэг. Тиймээс хяналтын үе шат нь холбогдох оролцогч талуудад эрсдэлийн талаар тайлагнах ажлыг эрчимжүүлдэг.

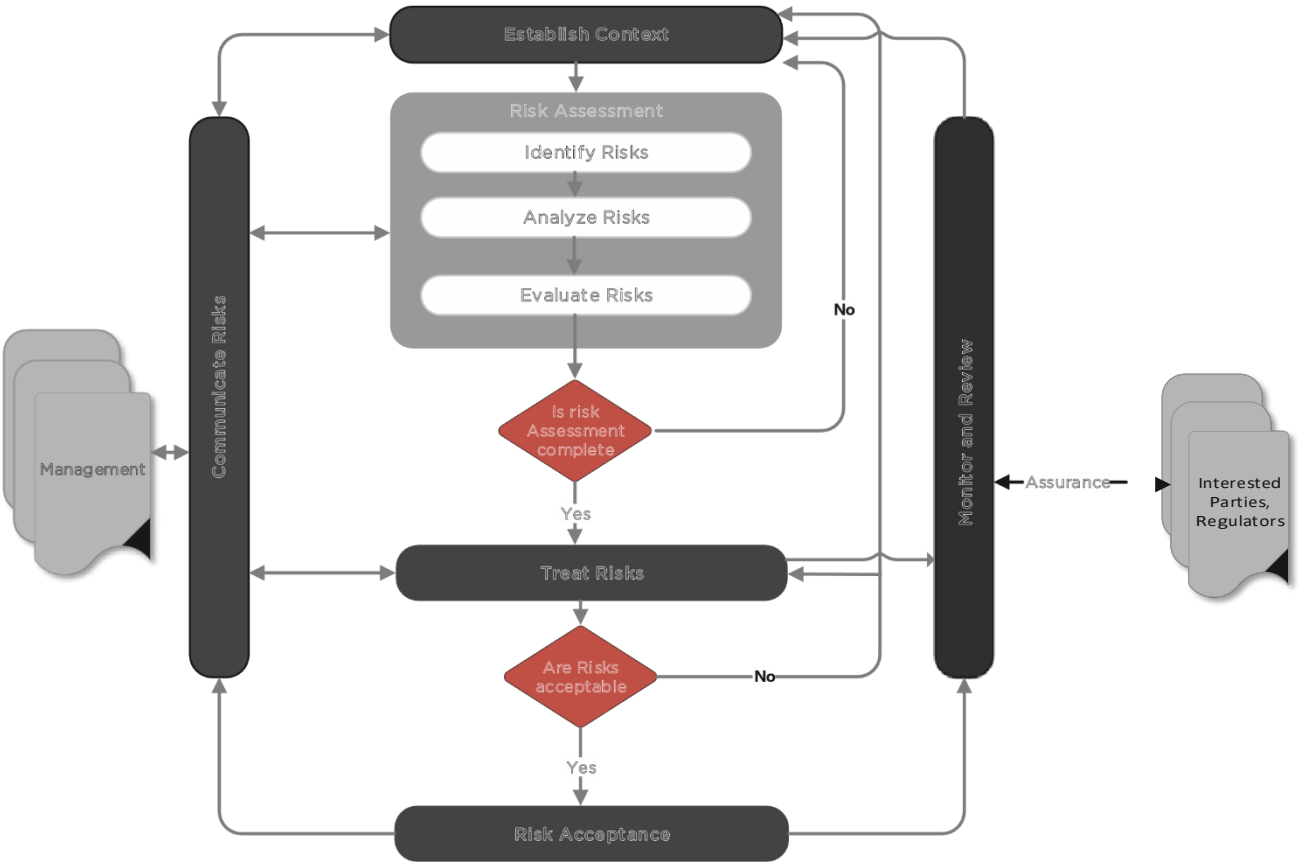
Эрсдэлийн удирдлагын үйл явцын бүх үе шатанд удирдлагатай харилцах нь нөхцөл байдлыг зөв тогтоох, эрсдэлийг зохих ёсоор тодорхойлох, олон талт эрсдэлийн шинжилгээ, үнэлгээ хийх гол үүрэг, хариуцлагыг ойлгож, эзэмшдэг. Удирдлагатай харилцах нь DFS-ийн бүх оролцогч талуудтай илүү өргөн хүрээтэй зөвлөлдөх, үйл явцын тойм хийх платформыг өгдөг бөгөөд энэ нь экосистемийн эрсдэлийг зохих, үнэн зөвөөр харах үндсэн дээр эрсдэлийн эмчилгээний төлөвлөгөөг батлах, дэмжлэг үзүүлэхэд тусалдаг.

Зураг 10 - Төлөвлөгөө, гүйцэтгэх, Шалгах, Үйлдэл



Өндөр түвшний эрсдэлийн удирдлагын үйл явцын төлөвлөгөөг доорх зурагт 11-д үзүүлэв. Энэ нь PDCA-ийн дөрвөн үе шатыг багтаасан болно.

Зураг 11 - Эрсдэлийн удирдлагын үйл явц



7.1. Хамрах хүрээ

DFS аюулгүй байдлын баталгааны хүрээ нь DFS экосистемийн оролцогч талуудад хамааралтай. Энэ нь дижитал хэрэгслээр санхүүгийн бүтээгдэхүүн, үйлчилгээг нийлүүлдэг DFS хэрэглэгчид, үүрэн холбооны операторууд, үйлчилгээ үзүүлэгчид, түүний дотор банкууд болон бусад лицензтэй банк бус санхүүгийн байгууллагуудын хэрэгжүүлэх аюулгүй байдлын хяналтыг тодорхойлдог; Эдгээр хяналтыг дижитал санхүүгийн үйлчилгээг боломжтой болгодог дэд бүтэц, программууд, төхөөрөмжүүд гэх мэтэд хэрэглэж болно.

Хэрэглэгчийн хувьд энэхүү хүрээ нь дижитал санхүүгийн үйлчилгээнд нэвтрэхэд ашигладаг гар утас гэх мэт төхөөрөмжүүдийн аюулгүй байдлын хяналтад төвлөрдөг. Хэрэгсэл, технологийг ихэвчлэн гар утасны сүлжээний оператор хангадаг бөгөөд энэ нь хэрэглэгч болон DFS үйлчилгээ үзүүлэгчийн хооронд холбоо тогтоох боломжийг олгодог бөгөөд уг хүрээ нь экосистемийг хамгаалахын тулд холбооны сүлжээний үйлчилгээ үзүүлэгч юу хийх ёстойг голчлон анхаардаг.

Энэхүү хүрээ нь банк эсвэл банк бус үйлчилгээ үзүүлэгч гэх мэт санхүүгийн байгууллага байж болох DFS үйлчилгээ үзүүлэгчийн тавих хяналтыг багтаасан бөгөөд зарим тохиолдолд харилцаа холбооны сүлжээний үйлчилгээ үзүүлэгч нь дижитал санхүүгийн үйлчилгээ үзүүлэгч байж болно.

7.2. Нөхцөл байдлыг бий болгох

Энэ нь эрсдэлийн удирдлагын үйл явцын эхний алхам бөгөөд оролцогч талууд DFS-ийн үйл ажиллагааны орчны талаар ойлголттой болох зорилготой юм. Үүнд эцсийн аюулгүй байдлыг хангах чадварт нөлөөлөх дотоод болон гадаад үйл явдлыг тодорхойлох шаардлагатай байдаг тул оролцогч талууд дижитал санхүүгийн үйлчилгээний үйл ажиллагаа явуулж буй дотоод болон гадаад нөхцөл байдлыг ойлгож, үнэлэх нь чухал бөгөөд энэ нь эрсдэлийн хамрах хүрээг тодорхойлоход тусалдаг. үнэлгээ.

Дотоод нөхцөл байдлыг бий болгохын тулд дараахь зүйлийг томъёолох шаардлагатай.

a. ISO/IEC 27001 стандартад суурилсан Мэдээллийн аюулгүй байдлын удирдлагын хүрээ нь норматив баримт бичгүүдийг авч үзэх буюу хэрэгжүүлэх ёстой.

b. DFS-ийн оролцогч талуудын байгууллагын ерөнхий бүтэц, DFS нь байгууллагын энэхүү бүтэц, түүний зорилгод хэрхэн нийцэж байгаа талаар үнэлэх.

c. DFS-ийн хөрөнгөд DFS-д хандахад ашигладаг туслах технологи, мэдээллийн систем, физик дэд бүтэц, програм хангамж, техник хангамж, агент сүлжээ, үйлчлүүлэгч/агент/худалдааны төхөөрөмжүүд орно.

d. Одоо байгаа дотоод хяналт, аюулгүй байдлын эрсдэлийн өмнөх үйл явдлууд, өмнөх залилангийн хэрэг, өмнөх аудитын тайлан, DFS төслийн баримт бичиг.

e. Зохицуулалтын шаардлага.

f. Эрсдэлд тэсвэртэй байдал, эрсдэлд орох байдал.

Бусад талуудын дунд гадаад нөхцөл байдал нь дараахь зүйлийг авч үздэг.

a. Санхүүгийн дижитал үйлчилгээтэй холбоотой хууль тогтоомж

b. DFS-ийн гол оролцогч талууд.

c. Улс төр, нийгмийн орчин, үүнд хүн амын боловсролын түвшин, гар утасны төхөөрөмжийн хэрэглээ, зорилтот бүлэгт ухаалаг утас нэвтрэх түвшин зэрэг хүн ам зүй орно.

d. Санхүүгийн дижитал үйлчилгээнд өрсөлдөх өөр хувилбарууд болон нэмэлт үйлчилгээнүүд.

e. Шинээр гарч ирж буй эрсдэлүүд ба тэдгээрийн санхүүгийн үйлчилгээ болон оролцогч талуудад үзүүлэх нөлөө.

Энэ үе шатны үр дүн нь цуглуулсан бүх мэдээллийн хураангуй хураангуй юм. Мэдээлэл нь эрсдэлийн үнэлгээний үйл явцад орц бүрдүүлнэ.

7.3. Аюулгүй байдлын үнэлгээ

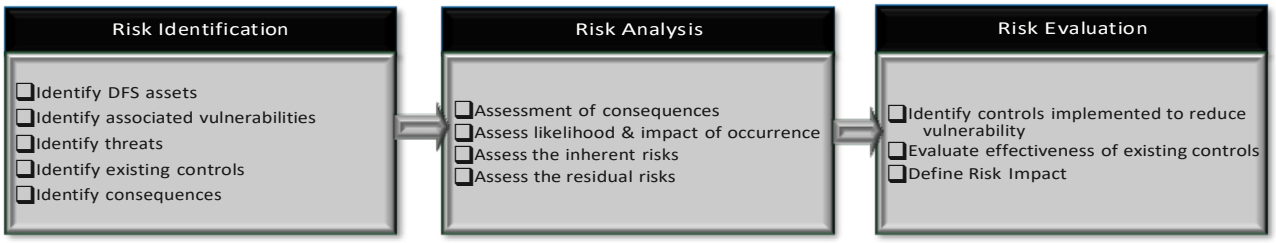
Эрсдэлийн үнэлгээ нь оролцогч талуудад DFS экосистемийн аюулгүй байдлын өнөөгийн түвшинг тодорхойлох арга хэмжээг авахад тусалдаг бөгөөд аюулгүй байдлын эрсдлийн үнэлгээний үйл явцад эрсдэлийг тодорхойлох, дүн шинжилгээ хийх, үнэлэх үйл явц орно. DFS-ийн эрсдлийн үнэлгээг үе үе хийж, үр дүнгийн талаар удирдлагад хариу өгөх ёстой.

Процессын үрсгалын тоймыг доор харуулав.

7.4. Эрсдэлийг тодорхойлох

Эрсдэлийг тодорхойлох нь DFS-ийн эмзэг байдлыг юу, хэрхэн, хаана, яагаад ашиглаж болохыг тодорхойлох явдал бөгөөд үүнд DFS-ийн чухал хөрөнгө, холбогдох аюул занал, эмзэг байдал, үүсэх магадлал, одоо байгаа хяналтын сул тал, нэгэнт ашиглагдсан аюул, сул талуудын нөлөөлөл, үр дагаврыг тодорхойлох шаардлагатай. Эрсдэлийг тодорхойлох явцад оролцогч тал дээрх 7.2-т заасан дотоод болон гадаад хүчин зүйлсийг мэдэж байх ёстой.

Зураг 12 - Эрсдэлийн үнэлгээний үйл явцын урсгал



Эрсдэлийг тодорхойлохдоо DFS-ийн оролцогч талууд таван чухал үйлдлийг анхаарч үзэх хэрэгтэй.

I. **Хөрөнгийн таних тэмдэг:** Энэ нь DFS экосистем дэх бүх хөрөнгийг жагсааж, хэн хариуцах вэ, DFS-ийн хөрөнгөд DFS-д хандахад ашигладаг физик дэд бүтэц, програм хангамжийн программ хангамж, техник хангамж, агентийн төхөөрөмж, үйлчлүүлэгч/агент/ худалдаачны төхөөрөмжүүд орно, гэхдээ үүгээр хязгаарлагдахгүй. үйлчилгээ болон холбооны сүлжээний төхөөрөмжүүд. Тодорхойлолт нь оролцогч талуудад DFS-ийн экосистемд учирсан ослын нөлөөнд үндэслэн DFS-ийн хөрөнгийг ангилах боломжийг олгодог бөгөөд ангилал нь DFS экосистемийн үнэ цэнэ, чухал байдалд үндэслэн хөрөнгийг ангилах зорилготой юм.

II. **Эмзэг байдлыг тодорхойлох:** эмзэг байдал нь эд хөрөнгөд халдах аюул заналхийлдэг сул тал эсвэл дутагдал бөгөөд эдгээрт зөвхөн бүтэцийн зохион байгуулалт, зохион байгуулалтын журам, боловсон хүчин, удирдлага, техник хангамж, програм хангамж, сүлжээ гэх мэт сул талууд орно, гэхдээ үүгээр хязгаарлагдахгүй. аюул заналхийллээр ашиглаж болох бөгөөд энэ нь системд гэмтэл, гэмтэл учруулж болзошгүй нөхцлүүд. Тодорхойлсон эмзэг байдлыг эрсдэлийн үнэлгээнд хөрөнгөнд нөлөөлж буй аюул заналхийллийг давхар тодотгох ёстой.

III. **Аюул заналыг тодорхойлох:** Аюул гэдэг нь тодорхой эмзэг байдлыг (санамсаргүй эсвэл санаатайгаар) ашиглах эх үүсвэр юм. DFS-ийн хөрөнгөд учирч болох аюул нь газар хөдлөлт, үер, хүний хулгай, залилан, техникийн жишээлбэл хортой программ хангамж, серверийн доголдол зэрэг байгалийн шинжтэй байж болно. Аюул заналхийлсэнийг илрүүлсний дараа аюул заналхийллээр ашиглаж болох аливаа эмзэг байдлыг илрүүлэхийн тулд мэдээллийн бүх төрлийг шинжлэх хэрэгтэй.

IV. **Одоо байгаа хяналтын тодорхойлолт:** одоо байгаа болон төлөвлөсөн бүх хяналтын жагсаалт, тэдгээрийн хэрэгжилт, ашиглалтын байдал.

V. **Үр дагаврыг тодорхойлох:** Эмзэг байдлыг амжилттай ашигласан осол эсвэл аюулын улмаас учирч болох хохирлын хэмжээ. Энэ үйл явц нь нөлөөлж болох хөрөнгө, нөлөөллийн ноцтой байдлыг тодорхойлдог. Ихэнх тохиолдолд DFS хөрөнгийн хохирлын хэмжээ нь энгийн солих зардлаас өндөр байдаг бөгөөд эдгээр нь мөнгө, техникийн, хүний болон зохицуулалттай холбоотой байж болох янз бүрийн хохирлыг харгалзан үздэг.

7.5. Эрсдэлийн шинжилгээ

Эрсдэлийн шинжилгээ нь хөрөнгөнд аюул учруулах магадлал, нөлөөллийн ерөнхий магадлалыг ойлгоход тусалдаг бөгөөд энэ нь шийдвэр гаргах, хамгийн чухал эрсдэл болон чухал эрсдэлийг (хамгийн их нөлөө үзүүлэх эрсдэл) шийдвэрлэх арга хэмжээг эрэмбэлэх зэрэгт чухал ач холбогдолтой юм. Эрсдэлийн шинжилгээний үр дүн нь эрсдэл бүрийн магадлал, нөлөөллийн зэрэглэлийг агуулсан эрсдэлийн шинэчилсэн бүртгэл юм. Эрсдэлийн шинжилгээг тоон болон чанарын хувьд эсвэл хоёуланг нь хослуулан хийж болно.

Дараах үйл явц нь эрсдэлийн шинжилгээний үе шатны үр дүн байх ёстой

I. Үр дагаврын үнэлгээ; Мэдээллийн аюулгүй байдлын болзошгүй буюу бодит ослын улмаас байгууллагад үзүүлэх бизнесийн нөлөөллийг мэдээллийн аюулгүй байдлын зөрчлийн үр дагаврыг, тухайлбал хөрөнгийн нууцлал, бүрэн бүтэн байдал, олдоц алдагдах зэргийг харгалзан үнэлнэ. Бусад зүйлсээс гадна DFS-ийн аюулгүй байдлын үр дагавар нь санхүүгийн алдагдал, нэр хүнд, зохицуулалтын хориг, торгууль зэрэг байж болно.

II. Эмзэг байдлыг ашиглаж болзошгүй аюул заналхийллийн магадлал, амжилттай болсон тохиолдолд түүний нөлөөллийг үнэл. Гарах магадлал нь урьдчилан сэргийлэх, мөрдлөг, хяналт, тэдгээрийн үр нөлөө, хэрэгжилт, ашиглалтыг харгалзан үзэх ёстой.

III. Төрөлхийн эрсдэлийн зэрэглэлийн магадлал ба нөлөөллийн бүтээгдэхүүн гэж тодорхойл. Төрөлхийн эрсдэлийн зэрэглэлийн зорилго нь хамгийн чухал эрсдэлийг шийдвэрлэхийн тулд удирдлагын арга хэмжээг эрэмбэлэхэд удирдлагад туслах явдал юм.

IV. Эрсдэлийг арилгах байгаа хяналтын үр нөлөөг үнэлэх замаар үлдэгдэл эрсдэлийг тодорхойлох. Хэрэгжүүлсэн хяналтууд DFS-ийн оролцогч талуудын эрсдэлийн дүршилд үндэслэн эрсдлийг хүлээн зөвшөөрөгдөх хэмжээнд хүртэл бууруулах ёстой.

7.6. Эрсдэлийн үнэлгээ

Эрсдэлийн үнэлгээний явцад DFS-ийн оролцогч талууд тодорхойлсон эрсдэлүүдийг харьцуулж, урьдчилан тодорхойлсон эрсдэлийн шалгуурын дагуу үнэлж, DFS экосистемд үзүүлэх эрсдэлийн цэвэр нөлөөг тодорхойлоход тусална. Үүнд одоо байгаа хяналтын үр нөлөөг тодорхойлох; өөрөөр хэлбэл, одоо байгаа хяналтуудыг авч үзсэний дараа эрсдэлийн магадлал, нөлөөллийг шинжлэх, дараа нь үлдэгдэл эрсдэлийг тооцоолох, энэ үйл явц нь эрсдэлийг эмчлэх, хэрэгжүүлэхтэй холбоотой тэргүүлэх ач холбогдол, шийдвэр гаргах боломжийг олгодог.

Эрсдлийн үнэлгээ хийхдээ дараахь зүйлийг анхаарч үзэх хэрэгтэй.

i. Хөрөнгийн ангиллын аюулын эмзэг байдлын хослол тус бүрд одоо байгаа хяналтын үр нөлөөг тодорхойлох, өөрөөр хэлбэл аюулын эмзэг байдлын хосолмол байдлыг багасгахад чиглэсэн хяналтын үр нөлөөг тодорхойлох.

ii. Эрсдлийн нөлөөллийг тодорхойлох

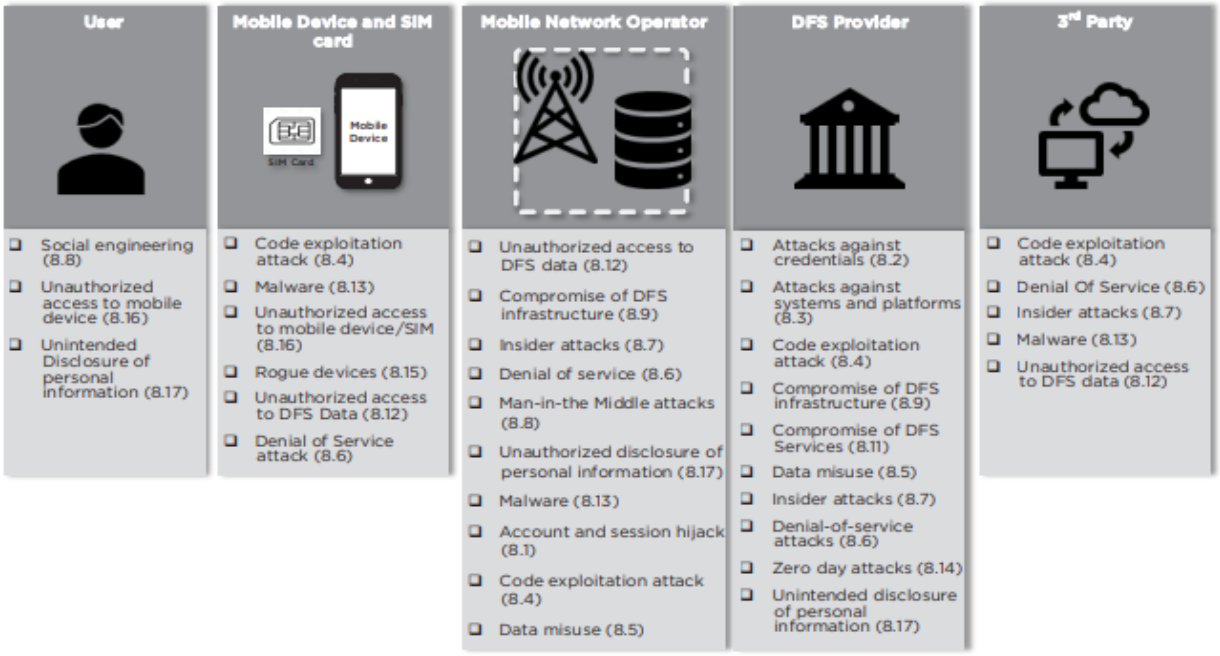
iii. Эрсдэл үүсэх магалдад зэрэглэлийг зэрэгцүүлэн үнэлэн тодорхойлно

8. DFS-ийн АЮУЛГҮЙ БАЙДЛЫН СУЛ ТАЛ, АЮУЛ ЗАНАЛ, АЮУЛГҮЙ БАЙДЛЫН ҮНЭЛГЭЭ, АВЧ ХЭРЭГЖҮҮЛЭХ АРГА ХЭМЖЭЭ

Дээрх хэсгүүдэд тодорхойлсон DFS экосистемд учирч бүй аюул занал, эмзэг байдлыг системтэйгээр эсэргүүцэхийн тулд бид төгсгөлийн аюулгүй байдлыг хангахад чиглэсэн аюулгүй байдлын найман хэмжигдэхүүн дээр тулгуурлан экосистемийн нэгж тус бүрд хяналт тавихыг санал болгож байна.

DFS экосистемийн хэмжээнд аж ахуйн нэгжүүдэд тулгарч бүй аюул заналхийллийн нийтлэг шинж чанарууд байдаг тул хэлэлцүүлгийг хөнгөвчлөхийн тулд эхлээд бидний тодорхойлсон стандарт аюул, ерөнхий аюулд өртсөн байгууллага, эмзэг байдлыг авч үзэх болно. холбоо, эрсдэл, санал болгож бүй бууруулах арга хэмжээ, тухайн аж ахуйн нэгжээс хэрэгжүүлж болох хяналтыг хянадаг. Бид эмзэг байдлыг ITU-T X.805 аюулгүй байдлын хэмжигдэхүүнд (SD) үзүүлэх нөлөөллийн хүрээнд байрлуулдаг.

Доорх зурагт үзүүлсэн диаграмм нь Зураг 9-д өмнө нь тодорхойлсон аюулгүй байдлын аюулыг доорх хэсгүүдэд тодорхойлсон аюулгүй байдлын хяналтын 119 арга хэмжээнд хэрхэн тусгасныг харуулж байна (тайлангийн хэсгийн дүгаар нь холбогдох хяналтыг хаана хэлэлцэхийг хаалтанд оруулсан болно).



8.1. Аюул: Бүртгэл болон сесс хулгайлах

Энд байгаа ерөнхий аюул бол халдагчийн данс эсвэл харилцааны сессийг хянах чадвар юм. Сул талууд нь DFS үйлчилгээ үзүүлэгч болон MNO дээр янз бүрээр илэрдэг.

Нөлөөлөлд өртсөн тал	Эрсдэл ба эмзэг байдал	Хяналт
DFS үйлчилгээ үзүүлэгч	**Мэдээлэлд өртөх, өөрчлөх** эрсдэл нь дараахь эмзэг байдлын улмаас үүсдэг. - Хэрэглэгчийн сешнүүдийн хяналт хангалтгүй (SD: хандалтын хяналт)	**C1:** DFS програмууд (логик сесс) дээр хэрэглэгчийн сессийг автоматаар гаргах, завсарлах хугацааг тохируулах. Аппликешн дотроос нууц үгийн нарийн төвөгтэй байдлыг хангах (серверээс хэрэгждэг), хамгийн их амжилтгүй нэвтрэх оролдлого, нууц үгийн түүх, дахин ашиглах хугацаа, акаунтыг хаах хугацааг боломжит хамгийн бага утгаар тохируулж, офлайн халдлагыг багасгах боломжтой.
	дансыг зөвшөөрөлгүй авах эрсдэл үүсдэг. - идэвхгүй дансны хяналт хангалтгүй (SD: баталгаажуулалт)	**C2:** Акаунтуудыг дахин идэвхжүүлэхийн өмнө идэвхгүй байгаа DFS акаунтын хэрэглэгчдэд хэрэглэгчийн таних баталгаажуулалтыг шаардах.
	Халдагчид эрх бүхий хэрэглэгчийн дүр эсгэх эрсдэл нь дараах сул талуудын улмаас үүсдэг.	
	- Газарзүйн байршлын баталгаажуулалтыг хийж чадаагүй (SD: Харилцаа холбооны аюулгүй байдал)	**C3:** Хэрэглэгчийн байршилд тулгуурлан DFS үйлчилгээнд хандах хандалтыг хязгаарлах (жишээ нь роуминг үед DFS USSD код, худалдаачид болон агентуудад STK болон SMS-д хандах хандалтыг идэвхгүй болгох) боломжтой бол DFS агентуудын хандалтыг бүс нутгаар нь хязгаарлах, боломжтой бол тухайн агент болон дугаарыг шалгах мөнгө байршуулах эсвэл мөнгө авах нь нэг үйлчилгээний бүсэд байна.
	- Хэрэглэгчийн сонгосон харилцааны сувгуудын хэрэглэгчийн баталгаажуулалт хангалтгүй DFS үйлчилгээнд зориулсан (SD: Харилцаа холбооны аюулгүй байдал)	**C4:** Харилцаа холбооны сувгаар DFS үйлчилгээг хязгаарлах (бүртгэлийн үеэр хэрэглэгчид үйлчилгээний хандалтын суваг, зөвхөн USSD, зөвхөн STK, зөвхөн апп эсвэл хосолмол сонголтоор сонгох ёстой) сонгосон сувгуудаар дамжуулан DFS хандалт хийхийг оролдсоныг хааж, улаан дарцагтай болгоно.
	Хэрэглэгчийн мэдээлэл болон эрхэд зөвшөөрөлгүй хандах эрсдэл нь дараах эмзэг байдлын улмаас үүсдэг.	

	- Таслагдсан жетон дээр суурилсан сессийг дахин тоглуулах (SD: харилцааны аюулгүй байдал)	**C5:** DFS систем нь үйлчлүүлэгчийн баталгаажуулалт эсвэл зөвшөөрлийн жетонд итгэх ёсгүй; хандалтын токенуудын баталгаажуулалтыг сервер талд хийх ёстой.
	- Нууц үг хадгалах сул шифрлэлтийн алгоритмууд (SD: мэдээллийн нууцлал)	**C6:** Хүчтэй давсалсан криптограф хэшлэх алгоритмуудыг ашиглан DFS нууц үгийг хадгалах.
MNO	**Зөвшөөрөгдсөн хэрэглэгчдийн дүрд хувирах** эрсдэл нь дараахь эмзэг байдлын улмаас үүсдэг. - DFS үйлчилгээнд сессийн завсарлага заагаагүй	**C7:** DFS үйлчилгээнд USSD, SMS, програм, вэб хандалтын сессийн завсарлага нэмнэ.
	Хэрэглэгчийн мэдээлэл болон эрхэд зөвшөөрөлгүй хандах эрсдэл нь дараах эмзэг байдлын улмаас үүсдэг. - DFS програмын хэрэглэгчийн эрхийг SMS эсвэл агентууд (SD: мэдээллийн нууцлал) гэх мэт найдвартай бус аргаар илгээдэг.	**C8:** Боломжтой бол DFS-ийн хэрэглэгчид бүртгүүлэхдээ нууц үгээ тохируулах ёстой бөгөөд DFS систем рүү дамжуулах бүх хугацаанд шифрлэгдсэн байх ёстой. Хэрэглэгчдэд анх удаа эрх(баталгаажсан) илгээсэн тохиолдолд DFS програмын эрхийг гуравдагч этгээд/агентгүйгээр шууд хэрэглэгчид илгээсэн эсэхийг шалгаарай. Хэрэглэгчид анх удаа нэвтэрсний дараа шинэ нууц үг оруулах шаардлагатай болно.

8.2. Аюул: Эрх(баталгаажсан нэвтрэх эрх)рүү халдсан

Бид эдгээр аюул заналхийллийг DFS систем болон хөдөлгөөнт төхөөрөмжүүдийн хэрэглэгчдийн эрхийг хулгайлах, өөрчлөх зорилготой гэж ерөнхийд нь тодорхойлдог.

Нөлөөлөлд өртсөн байгууллагууд	Эрсдэл ба эмзэг байдал	Хяналтууд
Гар утас	**Хэрэглэгчийн DFS акаунтыг зөвшөөрөлгүй нэвтрэх, авах** эрсдэл нь дараах сул талуудын улмаас үүсдэг.	
	- Програмын түвшинд сул нууц үг/ПИН ашиглах нь эдгээр баталгаажуулалтуудыг гадны халдлагад өртөмтгий болгодог (SD: нэвтрэлт танилт)	**C9:** Мобайл мөнгөний хэрэглээний программуудад илүү урт, таахад хялбар PIN/нууц үг ашиглахыг шаардах. Нарийн төвөгтэй ПИН ашиглахыг шаардахаасаа өмнө болгоомжтой байх хэрэгтэй; Хэт нарийн төвөгтэй ПИН кодыг бусад хүмүүс бичиж авах эсвэл оруулах, улмаар тэдний аюулгүй байдлыг доройтуулж болзошгүй тул ийм үрчлэх нь хэрэглэгчийн боловсролтой зэрэгцэн явагдах эсэхийг шалгаарай.
	- Хөдөлгөөнт төхөөрөмжид нэвтрэх энгийн ПИН ашиглах (SD: баталгаажуулалт)	**C10:** Төхөөрөмжийн өмчлөлийг харуулахын тулд найдвартай баталгаажуулалтын механизмуудыг ашиглана уу. ПИН-н түлхүүрийн зай нь тэднийг харгис хүчний халдлагад өртөмтгий болгодог тул илүү урт PIN буюу амархан санахад хялбар нэвтрэх үг зэрэг үсэг, тоон ПИН ашиглах талаар бодож үзээрэй.
	Man in the Middle халдлагуудаар дамжуулан эрх хулгайлах эрсдэл нь дараах эмзэг байдлаас шалтгаалж байна. - Серверийн буруу тохиргоо (SD: баталгаажуулалт)	**C11:** DFS програмууд нь тэдний холбогдож бүй серверийн нэрийг шалгах зориулалттай байх ёстой.
DFS үйлчилгээ үзүүлэгч	**DFS системийн эвдрэлийн** эрсдэл нь дарааҳь эмзэг байдлаас шалтгаална. - Нэвтрэх хяналтыг хийхгүй байх нь системийг харгис хүчний халдлагад өртөмтгий болгодог (SD: хандалтын хяналт)	**C12:** DFS систем (мэдээллийн сан, үйлдлийн систем, програм) дээрх арын хэрэглэгчид, худалдаачид, агентууд болон DFS хэрэглэгчдийн DFS данс руу нэвтрэх оролдлогын дээд хэмжээг хэрэгжүүлэх

8.3. Аюул: Систем болон платформуудын эсрэг халдлага

Бид эдгээр халдлагыг алсаас дотоод эрх мэдэл, бусад давуу эрхгүйгээр мэдээллийг тагнаж, өөрчлөх зорилгоор хийж болох халдлагууд гэж тодорхойлдог.

Нөлөөлөлд өртсөн тал	Эрсдэл ба эмзэг байдал	Хяналтууд
Гар утасны хэрэглэгч	**Хэрэглэгчийн төхөөрөмжөөс нэвтрэх эрхийг тагнах, алсаас хулгайлах** эрсдэл нь дараах эмзэг байдлаас шалтгаална.	
	- Баталгаажаагүй хортой хоёртын SMS SIM шинэчлэлтүүд (SD: баталгаажуулалт)	**C13:** Гар утасны хэрэглэгчийг хоёртын системд суурилсан SMS мессежүүдэд итгэх эсвэл үл итгэх боломжийг олгох. Ингэснээр SIM картанд хортой шинэчлэлт хийхээс сэргийлж чадна
MNO	- Хэрэглэгчийн нэвтрэх эрхийг баталгаатай шилжүүлэх (SD: хандалтын хяналт)	**C14:** DFS үйлчилгээ үзүүлэгчид хэрэглэгчийн баталгаажуулалтын эрхийг өөр сувгаар (хамтаас гадуур) найдвартай дамжуулах ёстой.
	Бүртгэлд нэвтрэх, нууцлалыг алдагдуулах , үйлчилгээ үзүүлэхээс татгалзах эрсдэл нь дараах эмзэг байдлаас шалтгаална. - Дотоод сүлжээг гадны халдагчдад өртөх (SD: хандалтын хяналт)	**C15:** DFS IP хаяг болон чиглүүлэлтийн мэдээллийн гадаад өртөлтийг хязгаарлахын тулд Сүлжээний хаягийн орчуулгыг ашиглана уу.
DFS үйлчилгээ үзүүлэгч	**Бүртгэлд нэвтрэх, зөвшөөрөлгүй болох , үйлчилгээ үзүүлэхээс татгалзах зэрэг** эрсдэлүүд нь дараах эмзэг байдлаас шалтгаална. - Дотоод системийг гадны халдагчдаас хамгаалах хамгаалалт хангалтгүй (SD: хандалтын хяналт)	**C16:** DFS системийг бусад бүх дотоод болон гадаад системүүдээс логикоор тусгаарладаг DMZ-ийг тохируулснаар DFS backend системд гадны системүүд шууд нэвтрэхээс зайлсхий.

8.4. Аюул: Код ашиглах халдлага

Бид эдгээр халдлагуудыг DFS программуудаас бүрдсэн код руу чиглэсэн халдлагууд гэж тодорхойлдог.

Нөлөөлөлд өртсөн байгууллага	Эрсдэл ба эмзэг байдал	Хяналт
DFS үйлчилгээ үзүүлэгч	**DFS** -ийн эрсдэл **Хэрэглээний** эвдрэл нь дараах эмзэг байдлаас үүдэлтэй: - DFS аппликейшн нь үйл ажиллагаа явуулж буй аюулгүй байдлын сангуудад найдах систем (SD: холбооны аюулгүй байдал)	**C17:** Үйлдлийн системээс санал болгож буй аюулгүй байдлын номын санг зөв зохиож, хэрэгжүүлсэн, тэдгээрийн дэмждэг шифрийн иж бүрдэл нь хангалттай хүчтэй байгаа эсэхийг шалгаарай.

8.5. Аюул: Мэдээллийг буруугаар ашиглах

Бид энэ аюулыг хэрэглэгчийн нууц мэдээлэлтэй бүруу харьцсантай холбоотой гэж тодорхойлдог [4].

Нөлөөлөлд өртсөн байгууллага	Эрсдэл ба эмзэг байдал	Хяналтууд
MNO	*Хэрэглэгчийн мэдээлэлд* **зөвшөөрөлгүй нэвтрэх** , **дамжих явцад мэдээлэл саатуулах** эрсдэл нь дараах эмзэг байдлаас шалтгаална. - Шифрлэлтийн сул практик эсвэл SMS, USSD (SD: харилцааны аюулгүй байдал) гэх мэт аюулгүй замын сувгуудаар тодорхой текстээр нууц мэдээллийг илгээх.	**C18:** Сүлжээгээр дамжин өнгөрөх болон өгөгдөл амарч байх үед PIN болон нууц үг зэрэг хэрэглэгчийн бүх нууц мэдээллийг шифрлэсэн эсэхийг шалгаарай.
DFS үйлчилгээ үзүүлэгч ба гуравдагч талын үйлчилгээ үзүүлэгч	**Эмзэг мэдээлэлд өртөх эрсдэл** нь дараахь эмзэг байдлаас шалтгаална.	
	- Өгөгдлийн хамгаалалтын хяналт хангалтгүй (SD: нууцлал)	**C19:** Хэрэглэгчийн мэдрэмтгий мэдээллийг ул мөрийн бүртгэлээс устгана уу. Хасах ёстой өгөгдлийн жишээнд бэлэн мөнгө авах эрхийн бичгийн код, банкны дансны дугаар, баталгаажуулалт орно. Үүний оронд боломжтой бол энэ өгөгдлийг бүртгэлд харуулахын тулд газар эзэмшигчийг ашиглана уу.
	- Гүйлгээ хийх явцад эсвэл API (SD: нууцлал) - аар дамжуулан хэрэглэгчийн нууц мэдээллийг ил гаргах.	**C20:** DFS үйлчилгээ үзүүлэгчид мэдээлэл хуваалцахыг зөвхөн гуравдагч этгээд болон үйлчилгээ үзүүлэгчтэй хийх гүйлгээнд шаардагдах хамгийн бага хэмжээгээр хязгаарлах ёстой.
	- API интерфейс дээрх сул шифрлэлт (SD: нууцлал)	**C21:** API-ийн хэрэглээг хянаж, гуравдагч этгээдтэй хуваалцсан бүх өгөгдлийг шифрлэх. Нэмж дурдахад, мэдээлэл/мэдээлэл алдагдахаас зайлсхийхийн тулд төлбөрийн үйлчилгээ үзүүлэгч нартай нууц задруулахгүй байх гэрээнд гарын үсэг зурсан гэх мэт өгөгдлийн удирдлагын журам, хяналтыг хэрэгжүүлнэ үү.

8.6. Аюул: Үйлчилгээг үгүйсгэх халдлага

Бид эдгээр халдлагыг DFS экосистемийн үйлчилгээг санал болгохоос урьдчилан сэргийлэх зорилготой гэж тодорхойлдог.

Нөлөөлөлд өртсөн байгууллага	Эрсдэл ба эмзэг байдал	Хяналтууд
MNO	**Үйлчилгээний тасалдлаас болж гүйлгээ хийх боломжгүй болох** эрсдэл болон **гүйлгээний саатал ихэссэний улмаас гүйлгээ бүтэлгүйтэх** нь дараах эмзэг байдлаас шалтгаална.	
	- Сүлжээний хүчин чадал хангалтгүй, засвар үйлчилгээ, дизайн зэргээс шалтгаалан сүлжээний доголдол (SD: бэлэн байдал)	**C22:** Үүрэн холбооны оператор нь USSD, SMS, интернетээр дамжуулан DFS үйлчилгээнд нэвтрэх боломжийг олгохын тулд сүлжээний өндөр сүлжээний хүртээмжийг хангах арга хэмжээ авах ёстой.

		C23: MNO нь системийн тасралтгүй ажиллагааг хангахын тулд хэрэглэгчийн тоо, хүлээгдэж буй өсөлт, хүлээгдэж буй гүйлгээний тоо, хүлээгдэж буй оргил үе зэрэгт үндэслэн өөр өөр гүйлгээг дуурайлган техникийн чадавхийн туршилт хийх ёстой.
DFS үйлчилгээ үзүүлэгч	- Сүлжээний траффик болон бие даасан сүлжээний багцын хяналт дутмаг (SD: хүртээмж, харилцааны аюулгүй байдал)	**C24:** DFS үйлчилгээ үзүүлэгч нь галт хана болон траффик шүүлтүүр ашиглан сүлжээний халдлагаас хамгаалж, CAPTCHA гэх мэт сүлжээнд нэвтрэх арга техник, механизмаар сэжигтэй урсгалыг сорьж DFS дэд бүтцийн аюулаас хамгаалах ёстой.
	Хэрэглэгчийн мэдээлэлд **зөвшөөрөлгүй нэвтрэх** эрсдэл нь дараахь эмзэг байдлаас үүдэлтэй. - Шаардлагагүй үйлчилгээг идэвхжүүлэх (SD: мэдээллийн нууцлал)	**C25:** Ирж буй интернетийн урсгалыг хязгаарлаж, байнга хянаж байх ёстой.
		C26: Галт ханын хязгаарлалттай дүрмийг анхдагчаар тохируулж, портуудыг цагаан жагсаалтад оруулах, пакет шүүлтүүрийг ашиглах, зөвшөөрөгдсөн/зөвшөөрөгдсөн портууд болон IP-д хандах хандалтыг тасралтгүй хянах.

8.7. Аюул: Дотор талын халдлага

Бид эдгээр халдлагыг байгууллагын периметр доторх, ихэвчлэн нөөцөд хандах эрх, давуу эрх бүхий халдлагчид хийдэг гэж тодорхойлдог.

Нөлөөлөлд өртсөн байгууллага	**Эрсдэл ба эмзэг байдал**	**Хяналтууд**
DFS үйлчилгээ үзүүлэгч	**Мэдээлэлд өртөх, өөрчлөх** эрсдэл дараах эмзэг байдлаас үүдэлтэй:	
	- Чухал үйл ажиллагааны дотоод хяналт хангалтгүй (SD: хандалтын хяналт)	**C27:** Боломжтой бол администратор өөр администраторын бүртгэл үүсгэх, өөрчлөх, устгах, өөрчлөх, хавсаргах, салгах зэрэг чухал үйлдлүүдэд (гэхдээ үүгээр хязгаарлагдахгүй) *дөрвөн нүдтэй зарчмыг (бүтээгч-шалгагч/хоёр хүний дүрэм) ашиглан чухал өөрчлөлтүүдийг хязгаарлаарай.* гар утасны дугаар/хэрэглэгчийн ID-аас DFS данс, гүйлгээг буцаах.
	- Өгөгдлийн оролтын баталгаажуулалт дутмаг (SD: мэдээллийн бүрэн бүтэн байдал)	**C28:** DFS үйлчилгээ үзүүлэгчид үйлдвэрлэгч-батлагчийн үүрэг хариуцлагыг хангалттай түсгаарлах ёстой; жишээ нь администраторт DFS бүртгэл үүсгэх болон идэвхжүүлэх эрх байхгүй байж болно.
	- Зөвшөөрлийн удирдлага хангалтгүй (SD: хандалтын хяналт)	**C29:** DFS-ийн эмзэг дэд бүтцэд физик хандалтыг хязгаарлах, хянах, хянах. Бусад дэд бүтцээс DFS дэд бүтцэд саад болох логик болон физик саад тотгорыг физикийн хувьд тусгаарлаж, байрлуулна. Урьдчилан сэргийлэх хандалтыг зөвхөн эрх бүхий хүмүүст л зөвшөөрч, илрүүлж, хэрэгжүүлснээр (жишээ нь албадан тохиолдолд дохиолол) солигддог хамгийн бага давуу эрх бүхий техникийг ашиглах. Бүх хандалтыг бүртгэх замаар системийн үйл ажиллагааг хянах (жишээлбэл, хэн хандсан, юунд хандсан, хаанаас хандсан, хэзээ хандсан).

(үргэлжлэл)

Нөлөөлөлд өртсөн байгууллага	Эрсдэл ба эмзэг байдал	Хяналтууд
DFS үйлчилгээ үзүүлэгч	Дараах эмзэг байдал нь **өгөгдлийн алдаа, зөрчилтэй байх эрсдэлийг үүсгэдэг** .	**C30:** DFS үйлчилгээ үзүүлэгч нь гадна талын үйлчилгээнүүдэд хязгаараас гадуурх утгууд болон зөвшөөрөгдөөгүй тэмдэгтүүдийг шалгаж, оролтыг хязгаарлаж, ариутгах замаар найдвартай оролтын баталгаажуулалтын горимуудыг ашиглах ёстой. Оролтын баталгаажуулалтыг аль болох эрт хийх ёстой бөгөөд үйлчлүүлэгч болон серверийн аль алинд нь хийх ёстой, гэхдээ сервер нь зөвхөн үйлчлүүлэгчийн баталгаажуулалтад найдах ёсгүй. Нэмж дурдахад вэб үйлчилгээний тайлбар хэл (WSDL) болон схемийг зөрчсөн бүх хүсэлтийг блоклож, бүртгэж, хянана.
	- Туршилтын өгөгдлийг үйлдвэрлэлийн өгөгдөлд нэмэх (SD: мэдээллийн бүрэн бүтэн байдал)	**C31:** Мэдээллийн сангийн хуруугны хээг ашиглан өгөгдөл хадгалагдсаны дараа хөндлөнгөөс оролцох, өөрчлөхийг илрүүлэх. Хэрэглэгчийн өгөгдлийн өөрчлөлтийг илрүүлэхийн тулд өгөгдлийн сангийн багана дээрх тоон гарын үсэг зэрэг техникийг ашиглаж болно.
		C32: Бүх туршилтын өгөгдлийг үйлдвэрлэлийн орчинд шилжүүлэхээс өмнө кодоос устгасан эсэхийг шалгаарай.
	- Бүртгэл байхгүй, бүртгэлийг өөрчлөх чадваргүй, бүртгэл дэх мэдээлэл хангалтгүй (SD: үгүйсгэхгүй)	**C33:** DFS системүүд нь хэрэглэгчийн үйлдлийн гарал үүслийг олж авах эсвэл чухал үйлдлүүдийг хөндлөнгийн хамгаалалттай хадгалах санд бүртгэх, DFS системийн бүртгэлийг хөндлөнгөөс оролцох, засварлах, устгах, зогсоохоос хамгаалах зэрэг бүртгэлийн механизмуудыг ашиглах ёстой. Үйлдлүүд, ялангуяа сүлжээний холболтоор ирдэг тоон гарын үсгийг ашиглана уу.
	- Нарийвчлалгүй , синхрончлогдоогүй цаг (SD: мэдээллийн бүрэн бүтэн байдал)	**C34:** DFS системд холбогдсон бүх систем дээр цагийн нарийвчлалын синхрончлолыг баталгаажуулах. NTP болон SNTP нь үнэн зөв цагийг синхрончлоход ашигладаг зарим протоколууд юм; Гэсэн хэдий ч эдгээрийг найдвартай байрлуулах ёстой.

8.8. Аюул: Дундын халдагч ба сошиал инженерчлэлийн халдлага

Бид эдгээр хоёр төрлийн халдлагыг бүлэглэв, учир нь эдгээр нь хоёулаа халдагч, харилцаа холбоо, харилцан үйлчлэлд (жишээлбэл, хэрэглэгч ба төхөөрөмж эсвэл MNO хооронд, эсвэл талуудын хооронд харилцаа холбоо) идэвхтэй оролцох явдал юм.

Нөлөөлөлд өртсөн байгууллага	Эрсдэл ба эмзэг байдал	Хяналтууд
Гар утасны хэрэглэгч	**Мэдээлэлд өртөх, өөрчлөх** эрсдэл дараах эмзэг байдлаас үүдэлтэй:	
	- Баталгаажаагүй, гарын үсэг зураагүй програмууд (SD: нууцлал, мэдээллийн бүрэн бүтэн байдал)	**C35: Хортой** програмаар халдварласан апп-уудыг ажиллуулах эрсдэлийг бууруулахын тулд хэрэглэгчийг албан ёсны програмын хувилбарын сувгуудаар дамжуулан DFS програмуудад хандах, татаж авахад чиглүүлэхэд онцгой анхаарал хандуулах хэрэгтэй.
	- Хүсэгүй SMS мессеж, апп доторх зар сурталчилгаа, и-мэйл гэх мэт баталгаажуулаагүй оролт (SD: мэдээллийн бүрэн бүтэн байдал)	**C36:** MNO болон DFS үйлчилгээ үзүүлэгчид хэрэглэгчид болон дотоод ажилтнуудад хортой мессеж, фишинг халдлага, хууран мэхлэлтийн талаар мэдлэг олгохын тулд үйлчлүүлэгчдийг таниулах идэвхтэй кампанит ажил явуулах ёстой.
	- Хангалтгүй хамгаалагдсан баталгаажуулалтууд (SD: хандалтын хяналт)	**C37:** Хэрэглэгчийн нууц үг болон ПИН кодыг далдалж, мөрөн дээр серфинг хийх, нууц үгээ бичихээс зайлсхийхийн тулд хэрэглэгчдийг мөрөн дээр серфинг хийх, аюулгүй ПИН/нууц үг ашиглах талаар идэвхтэй сургах.

(үргэлжлэл)

Нөлөөлөлд өртсөн байгууллага	Эрсдэл ба эмзэг байдал	Хяналтууд
MNO	**Хэрэглэгчийн мэдээлэлд зөвшөөрөлгүй хандах** эрсдэл нь дараах эмзэг байдлаас шалтгаална. - Агаараар дамжуулах сул шифрлэлт (SD: холбооны аюулгүй байдал)	**C38:** A5/0, A5/1, болон A5/2 GSM шифрлэлтийн шифрийг ашиглахаа болих. A5/3 болон A5/4-ийг эвдэх боломж, хялбар байдлын талаар аюулгүй байдлын болон криптографийн нийгэмлэгийн үр дүнг сайтар хянаж, илүү хүчтэй шифрүүдийг авч үзэх хэрэгтэй. Эдгээр шинэ шифрүүдэд байршуулах стратегийг бэлэн болго.
	Хэрэглэгчийн дүрд хувирах эрсдэл нь дараах эмзэг байдлаас шалтгаална. - Дуудлагын шугамыг тодорхойлох шүүлтүүр сул (SD: холбооны аюулгүй байдал)	**C39:** MNO нь DFS үйлчилгээ үзүүлэгчийн дуудлага шиг хуурамчаар үйлдэгдэж болзошгүй дуудлага, мессежийг илрүүлэхийн тулд дуудлага/SMS-д CLI шинжилгээ хийх ёстой.
DFS үйлчилгээ үзүүлэгч	**Хэрэглэгчийн дансны авах** эрсдэл нь дараахь эмзэг байдлаас үүдэлтэй. - Дансны тохиргоо болон зөвшөөрлийн хяналт дутуу/хангалтгүй байна (SD: баталгаажуулалт)	**C40:** Өндөр эрсдэлтэй дансны өөрчлөлт, гүйлгээнд хэрэглэгчийн баталгаажуулалт, зөвшөөрлийг шаардаж, төхөөрөмж нэвтэрсэн байсан ч PIN эсвэл нууц үгийн талаарх мэдлэгийг харуулах хүртэл гүйлгээ хийхээс татгалзах.
Гуравдагч этгээдийн үйлчилгээ үзүүлэгчид	**Нууц мэдээлэлд өртөх** эрсдэл нь дараахь эмзэг байдлаас шалтгаална.	
	- Төхөөрөмжид хадгалагдсан өгөгдөл болон дамжуулсан өгөгдөлд ашигладаг сул шифрлэлтийн алгоритмууд (SD: нууцлал)	**C41:** Хөдөлгөөнт аппликейшн доторх өгөгдлийг хамгаалах, арын DFS системтэй харилцах аль алинд нь хангалттай аюулгүй шифрлэлтийг ашиглах ёстой бөгөөд боломжтой бол хэрэглэгчийн нууц мэдээллийг далдлах, тайрах, өөрчлөх шаардлагатай.
	- Харилцаа холбооны шифрлэлт дутмаг (SD: холбооны аюулгүй байдал)	**C42:** Гүйлгээ хийх үед DFS системд холбогдсон гуравдагч этгээдийг тодорхойлохын тулд тоон гарын үсгийг ашиглана.
	- Сертификат эсвэл гол материалын менежмент хангалтгүй (SD: хандалтын хяналт)	**C43:** DFS үйлчилгээ үзүүлэгч болон гуравдагч этгээдийн хооронд өгөгдөл солилцохыг зөвшөөрөхийн тулд зөвхөн баталгаажсан түлхүүр болон баталгаажуулалтыг хүлээн авах ёстой бөгөөд тэдгээрийг задруулахаас хамгаална.
	хулгайлах, бүтэлгүйтсэн гүйлгээний эрсдэл нь дараахь эмзэг байдлаас шалтгаална. - DFS үйлчилгээ үзүүлэгч эсвэл MNO системийн алдаа нь агентууд/гуравдагч этгээдүүдийг офлайн процесс руу буцаахад хүргэдэг (SD: бэлэн байдал)	**C44:** Холбогдох үйлчилгээ үзүүлэгчтэй систем сул зогсолтын үед үр дүнтэй удирдах процедурын болон техникийн хяналтыг тохируулна уу. Жишээлбэл, DFS системд нэвтрэх тасалдалтай үед офлайн гүйлгээг (жишээ нь, SIM солих) удирдах хяналтыг тохируулна уу. DFS систем эсвэл гуравдагч талын системийн хандалт тасалдсан үед мөнгөн гүйвуулга болон гуравдагч этгээдийн төлбөрийг шалгах нэмэлт шалгалт хийнэ үү.

8.9. Аюул: DFS дэд бүтцийн эвдрэл

Бид эдгээр халдлагуудыг DFS экосистемийн үндсэн дэд бүтцэд чиглэсэн гэж тодорхойлдог.

Нөлөөлөлд өртсөн байгууллага	Эрсдэл ба эмзэг байдал	Хяналтууд
DFS үйлчилгээ үзүүлэгч	-ийн эрсдэл **дэд бүтэц, мэдээллийн эвдрэл** дараах эмзэг байдлаас шалтгаалж байна: - Хэрэглэгчийн акаунт дээрх аюулгүй, хангалтгүй хандалтын хяналт (SD: хандалтын хяналт)	**C45:** DFS бүртгэлд хандахын тулд олон хүчин зүйлтэй эсвэл олон загварын баталгаажуулалтыг ашиглана уу.

(үргэлжлэл)

Нөлөөлөлд өртсөн байгууллага	Эрсдэл ба эмзэг байдал	Хяналтууд
DFS үйлчилгээ үзүүлэгч	**Үйлчилгээ тасрах, гүйлгээ хийх боломжгүй болох** эрсдэл нь дараахь эмзэг байдлаас шалтгаална. - Түршилтанд ороогүй сэргээн засварлах арга (SD: бэлэн байдал)	**C46:** Үйлдвэрлэлийн DFS системтэй харьцдаг мэдээллийн сан, программ, үйлдлийн систем болон бусад хандалтын интерфейсээс анхдагч бүртгэл, баталгаажуулалтыг идэвхгүй болгож, устгана.
		C47: Суурилуулалт, борлуулагч, дэмжлэгийн бүртгэл, DFS систем болон дэд бүтцэд нэвтрэх цэгүүдийг шалгана уу. Эдгээр бүх бүртгэлийг идэвхгүй болгох эсвэл зохих хэрэглэгчийн профайлд хуваарилах ёстой.
	Мэдээллийг задлах, өөрчлөх, гүйлгээний бүрэн бүтэн байдлыг алдагдуулах, үйлчилгээний **тасалдал зэрэг** эрсдэлүүд дараах эмзэг байдлаас үүдэлтэй: - Гүйлгээний атомын шинж чанарыг хэрэгжүүлэхгүй байх, тэдгээрийг хэсэгчлэн дууссан төлөвт байлгах зэрэг мэдээллийн хангалтгүй хяналт (SD: мэдээллийн бүрэн бүтэн байдал)	**C48:** DFS, MNO, SP болон гуравдагч этгээдийн системд гарсан аливаа өөрчлөлтийн дараа төгсгөл хүртэлх туршилтыг хийж, регресс болон хүчин чадлын туршилтыг хүлээн авах туршилтанд оруулна. Түүнчлэн, буцаах/харах төлөвлөгөө байгаа эсэхийг шалгаарай.
		C49: DFS системүүдийн хуваарьтай, тогтмол нөөцлөлттэй байх. Нөөцлөлтийг офлайн болон сайтаас гадуур шифрлэгдсэн хэлбэрээр тогтмол туршиж, найдвартай хадгалаарай.
		C50: Гүйлгээний бүрэн бүтэн байдлыг хангахын тулд мэдээллийн сангийн стандарт ACID (Atomicity, Consistency, тусгаарлах, бат бөх чанар) функцийг ашиглана уу. DFS үйлдлүүд нь бүрэн амжилттай эсвэл бүрмөсөн бүтэлгүйтэх ёстой. DFS үйлчилгээ үзүүлэгч нь давхардсан гүйлгээг (өвөрмөц гүйлгээ ID, цагийн тэмдэг, криптографийн хэрэглээ)
Гуравдагч этгээдийн үйлчилгээ үзүүлэгч	**Хэрэглэгч гүйлгээ хийх боломжгүй болох** эрсдэл дараах эмзэг байдлаас шалтгаалж байна: - Өгөгдлийн бүрэн бүтэн байдлыг хангах механизм хангалтгүй, гадаад итгэлцлийн зангуунд хэт найдах (SD: үгүйсгэхгүй)	**C51:** DFS програмууд/гуравдагч талууд тоон гарын үсгийн хэрэглээг дэмжих ёстой, найдвартай тоон гарын үсэг нь гүйлгээний гарал үүслийг үгүйсгэх аргагүй нотлох баримт болдог. Дижитал гарын үсэг нь PKI-д халдаагүй тохиолдолд л хүчинтэй бөгөөд авхаалж самбаагаа баталгаажуулах төлөвлөгөөний дагуу турших ёстой. Гарын үсэг зурах түлхүүрүүд нь үндсэн түлхүүр хүртэл зохих ёсоор хамгаалагдсан гэдгийг харуулснаар DFS үйлчилгээ үзүүлэгч нь тодорхой хэрэглэгч болон маргаантай гүйлгээний жинхэнэ байдлын талаарх хууль эрх зүйн сорилтуудыг даван туулж чадна.

Нөлөөлөлд өртсөн байгууллага	Эрсдэл ба эмзэг байдал	Хяналтууд
MNO	**Данс авах, зөвшөөрөлгүй гүйлгээ хийх** эрсдэл тохиолддог дараах эмзэг байдлын улмаас: - SIM солих болон SIM дахин боловсруулахаас өмнө хэрэглэгчийн таних, баталгаажуулах хяналт хангалтгүй (SD: Баталгаажуулалт)	**C52:** MNO нь SIM солихын өмнө хэн болохыг баталгаажуулах үйл явц байгаа эсэхийг баталгаажуулах ёстой.
		C53: Хэрэглэгчийн хэн болохыг өөрт байгаа зүйл, түүнд байгаа зүйл эсвэл мэддэг зүйлсийн хослолыг ашиглан баталгаажуулах ёстой. Жишээлбэл, SIM солих/Сим солихын өмнө хүчинтэй ID, биометрийн баталгаажуулалт, DFS дансны дэлгэрэнгүй мэдээллийг танилцуулах.
		C54: DFS болон Төлбөрийн үйлчилгээ үзүүлэгч нь DFS үйлчилгээ бүхий SIM картыг солих эсвэл солих бүрийг бодит цаг хугацаанд нь илрүүлэх боломжтой байх ёстой. Мөн шинэ SIM картаар өндөр дүнтэй гүйлгээ хийх эсвэл дансны өөрчлөлт оруулахаас өмнө нэмэлт баталгаажуулалт хийнэ үү.

8.10. Аюул: SIM-н халдлага

Ерөнхий аюул бол халдагчид DFS хэрэглэгчийн SIM карт руу зөвшөөрөлгүй нэвтрэх чадвар юм. Эмзэг байдал нь Үүрэн холбооны сүлжээний оператор, DFS үйлчилгээ үзүүлэгч, Мобайл хэрэглэгчдэд янз бүрээр илэрдэг.

Нөлөөлөлд өртсөн байгууллага	Эрсдэл ба эмзэг байдал	Хяналтууд
MNO	**Данс авах, зөвшөөрөлгүй гүйлгээ хийх** эрсдэл тохиолддог дараах эмзэг байдлын улмаас: - SIM солих болон SIM дахин боловсруулахаас өмнө хэрэглэгчийн таних, баталгаажуулах хяналт хангалтгүй (SD: Баталгаажуулалт)	**C55:** Мобайл оператор нь IMSI болон SIM нууц түлхүүрийн утгууд (KI утгууд) зэрэг SIM өгөгдлийг хамгаалж, найдвартай хадгалах ёстой.
		C56: Мобайл захиалагчийн таних дугаар (MSIDN)-ийг хаах эсвэл дахин боловсруулах талаар DFS үйлчилгээ үзүүлэгчидтэй харилцахтай холбоотой гар утасны дугаарыг дахин боловсруулах үйл явц байх ёстой. (энэ хүрээнд: дугаарын дахин боловсруулалт гэдэг нь MYO идэвхгүй/идэвхгүй байгаа гар утасны захиалагчийн дугаарыг (MSISDN) шинэ хэрэглэгч рүү дахин хуваарилах явдал юм). SIM картыг дахин ашиглах үед гар утасны оператор холбогдох дансны утасны дугаарын шинэ IMSI-г мэдээлэх болно. DFS үйлчилгээ үзүүлэгч нь SIM картыг эзэмшиж буй шинэ хүний данс эзэмшигч болохыг баталгаажуулах хүртэл дансыг хаах ёстой.
Гар утасны хэрэглэгч	**Хэрэглэгчийн гар утасны өгөгдөлд зөвшөөрөлгүй нэвтрэх** эрсдэл нь дараахь эмзэг байдлын улмаас үүсдэг. - Мобайл төхөөрөмжийн хулгай (SD: мэдээллийн нууцлал)	**C57:** DFS-ийн хэрэглэгчид гар утасны төхөөрөмж дээр алсын зайнаас арчих, төхөөрөмж алдагдсан эсвэл хулгайлагдсан тохиолдолд мэдээллээ шифрлэх чадвартай байх ёстой.
DFS үйлчилгээ үзүүлэгч	**Данс руу нэвтрэх эрхээ алдах эсвэл нэр хүндэд хохирол учруулах** эрсдэл нь дараахь эмзэг байдлын улмаас үүсдэг. - SIM солих, дахин боловсруулах үйл явцын хангалтгүй байдал [5] (SD: мэдээллийн бүрэн бүтэн байдал)	**C58:** DFS үйлчилгээ үзүүлэгчид сэжигтэй SIM солих болон SIM дахин боловсруулалтыг илрүүлэх, урьдчилан сэргийлэх журамтай байх ёстой: a) Утасны дугаартай холбоотой IMSI өөрчлөгдсөн эсэхийг шалгана уу, энэ нь SIM солих шинж тэмдэг юм. b) Хэрэв SIM солих шинж тэмдэг байгаа бол SIM барьж буй утасны IMEI-г шалгана уу. Хэрэв IMEI нь өөрчлөгдсөн бол SIM солих магадлал өндөр байна. Энэ тохиолдолд DFS үйлчилгээ үзүүлэгч нь жишээлбэл дуут дуудлага эсвэл агентаар дамжуулан данс баталгаажуулах процедурыг гүйцэтгэх хүртэл дансыг блоклох ёстой.

8.11. Аюул: DFS үйлчилгээний эвдрэл

Ерөнхий аюул нь халдагчийн санхүүгийн үйлчилгээг илрүүлэхгүйгээр зөрчих чадвар юм. DFS үйлчилгээ үзүүлэгч дээр эмзэг байдал өөр өөр хэлбэрээр илэрдэг

(үргэлжлэл)

Нөлөөлөлд өртсөн аж ахуйн нэгж	Эрсдэл ба эмзэг байдал	Хяналтууд
DFS үйлчилгээ үзүүлэгч	- Хэрэглэгчийн хандалтын баталгаажуулалт эсвэл хэрэглэгчийн оруулсан баталгаажуулалт хангалтгүй (SD: Баталгаажуулалт)	**C60:** Хэрэглэгч болон гуравдагч талын үйлчилгээ үзүүлэгчийн DFS системд хандахын тулд хүчирхэг олон хүчин зүйлийн баталгаажуулалтыг ашиглах , жишээ нь токен эсвэл биометр, системийн хэрэглэгчдийг баталгаажуулахын тулд олон хүчин зүйлийн баталгаажуулалтыг ашиглах нь гарал үүслийг үгүйсгэхгүй байдлыг нэмэгдүүлдэг.
		C61: Ирж буй өгөгдлийг API-тай холбоотой өгөгдлийн схемийн хүлээгдэж буй утгуудтай харьцуулж USSD-д шалгах, HTTP хүсэлтээр XML-ийн XML баталгаажуулалтыг хийх.
		C62: Хэрэглэгчийн гүйлгээ хоорондын хурд, өдрийн гүйлгээний цагийг шалгахын тулд аналитик системийг ашиглан зөвшөөрлийн баталгаажуулалтын нэмэлт шалгалтыг ашиглана уу.
		C63: Баримт бичгийг (и-мэйл, SMS эсвэл хавсаргасан хэвлэгч гэх мэт) гаргахад ашигладаг аргаас үл хамааран үг арга нь холбогдох хууль тогтоомж, дүрэм журам, төлбөрийн картын бодлогыг дэмжих үүднээс Үндсэн дансны дугаарыг (PAN) далдлах ёстой. Бодлого, практикийн дагуу DFS Үйлчилгээ үзүүлэгч/худалдаачин нь PAN эсвэл Мэдрэмжтэй баталгаажуулалтын өгөгдөл (SAD) илгээхийн тулд и-мэйл, SMS зэрэг аюулгүй бус сувгуудыг ашиглахыг зөвшөөрөх ёсгүй.

8.12. Аюул: DFS өгөгдөлд зөвшөөрөлгүй хандах

Ерөнхий аюул нь халдагчид DFS хэрэглэгчдийн DFS өгөгдөлд зөвшөөрөлгүй нэвтрэх боломж юм. Эмзэг байдал нь Үүрэн холбооны сүлжээний оператор, DFS үйлчилгээ үзүүлэгч болон Мобайл хэрэглэгчдэд янз бүрийн хэлбэрээр илэрдэг.

Нөлөөлөлд өртсөн аж ахуйн нэгж	Эрсдэл ба эмзэг байдал	Хяналтууд
DFS үйлчилгээ үзүүлэгч	**Үйлчилгээний доголдол, DFS үйлчилгээ, өгөгдөлд аюул учруулах** эрсдэл нь дараахь эмзэг байдлын улмаас үүсдэг.	
	- Системийн тохиргоо болон бүртгэлийн файл, өгөгдөлд зөвшөөрөлгүй өөрчлөлт оруулах (SD: Өгөгдлийн бүрэн бүтэн байдал)	**C59:** Хулгайлахаас хамгаалж, зөвхөн онлайн гүйлгээг зөвшөөрөх a) DFS програмын файлуудыг шалгах, тоон гарын үсгийг баталгаажуулах гэх мэт файлын бүрэн бүтэн байдлын монитор ашиглан хөндлөнгөөс оролцох, өөрчлөхөөс хамгаалж, хянаж болно. b) Бодлогын дагуу DFS үйлчилгээ үзүүлэгч эсвэл худалдаачин гар утасны төлбөрийн шийдлийг офлайнаар гүйлгээг зөвшөөрөх эсвэл дараа нь дамжуулах зорилгоор гүйлгээг хадгалахгүй байх ёстой.
	DFS хэрэглэгчийн гар утасны өгөгдөлд зөвшөөрөлгүй нэвтрэх эрсдэл дараах эмзэг байдлын улмаас үүсдэг.	
Гар утасны хэрэглэгч	- Хэрэглэгчийн бүртгэлд хандах хяналтын механизм хангалтгүй (SD: Хандалтын хяналт)	**C64:** DFS хэрэглэгчид өөрийн бүртгэлийн PIN кодоо тохируулах ёстой. Анх удаа PIN кодыг DFS үйлчилгээ үзүүлэгчийн систем эсвэл түүний агентууд тохируулсан тохиолдолд PIN код нь хэрэглэгч бүрийн хувьд өвөрмөц бөгөөд анх нэвтрэх үед ашиглалтын өөрчлөлтийг шаарддаг.

(үргэлжлэл)

	- Төхөөрөмж дээрх эмзэг өгөгдөлд хандах хязгаарлагдмал хяналт (SD: Хандалтын хяналт)	**C65** : DFS-ийн хэрэглэгчид хүчтэй нууц үгээ тохируулж, төрсөн өдөр гэх мэт төхөөрөмждөө амархан тааварлах зүү хэрэглэхээс зайлсхийх хэрэгтэй.
		C66: DFS-ийн эмзэг мэдээллийг хөдөлгөөнт төхөөрөмжийн аюулгүй хэсэгт хадгалсан эсэхийг шалгаарай.
		C67: Апп хөгжүүлэгчид төхөөрөмж дээр програм суулгахын өмнө хэрэглэгчийн баталгаажуулалт шаардлагатай эсэхийг шалгах ёстой.
		C68: Апп хөгжүүлэгчид DFS дэд бүтэц, аппликейшн болон үйлчилгээнд нэвтрэх эрхийг зөвхөн таниулах баталгаажуулалтын дараа л зөвшөөрөх ёстой. Олон хүчин зүйлийн баталгаажуулалтыг ашиглах, Хэрэглэгчийн мэддэг зүйл (PIN гэх мэт), Түүнд байгаа зүйл (Сим карт гэх мэт), Түүнд байгаа зүйл (хурууны хээ эсвэл бусад биометрийн арга гэх мэт).
		C69: Апп хөгжүүлэгчид DFS програмууд нь хандалтын баталгаажуулалтыг найдвартай удирдах ёстой.

Нөлөөлөлд өртсөн аж ахуйн нэгж	**Эрсдэл ба эмзэг байдал**	**Хяналтууд**
MNO	*дамжуулах явцад* **саатуулах** эрсдэл нь дараахь эмзэг байдлын улмаас үүсдэг.	**C70** : PIN код, нууц үг зэрэг хэрэглэгчийн бүх нууц мэдээллийг дотоод сүлжээн дэх хүчтэй шифрлэлтээр найдвартай хадгалж, энэ өгөгдлийн эсрэг дотоод аюулыг багасгахын тулд амарч байгаа эсэхийг шалгаарай.
	- SS7-ийн аюулгүй байдлын сул тал [6] (SD: Харилцаа холбооны аюулгүй байдал)	**C71:** SS7-ийн аюулгүй байдлын алдаан дээр үндэслэн халдлагыг илрүүлэх, хязгаарлахын тулд галт хана ашиглана уу.
	- MO-USSD гүйлгээг саатуулах (SD: Харилцаа холбооны аюулгүй байдал)	**C72:** Гүйлгээ хийж буй төхөөрөмжийн IMEI нь данс эзэмшигчийн утасны бүртгэлтэй IMEI-тэй таарч байгаа эсэхийг шалгана уу (MITM систем нь SIM-г өөр IMEI-ээр хуулбарлаж болно)
	- Хамгаалалтгүй эмзэг траффик ба шифрлэлтийн сул практик (SD: Харилцаа холбооны аюулгүй байдал)	**C73:** Гүйлгээ хийхэд ашигласан утасны байршлыг утасны хамгийн сүүлд мэдээлэгдсэн байршилтай (хамгийн сүүлд ирсэн/гарсан SMS эсвэл дуудлага) харьцуулж хэрэглэгчийн хурдыг хяна.
		C74: Хөдөлгөөнт төхөөрөмж алдагдсан, хулгайлагдсан тохиолдолд нэмэлт аюулгүй байдлын үүднээс MNO нь SIM карт дээрх Хувийн түгжээг тайлах түлхүүрийг (PUK) ашиглах ёстой.
		C75: USSD дээр MSC MAP мөрдөх болон протокол анализаторын ашиглалтыг хянах, хянах, энгийн текст SMS болон дамжин өнгөрөх USSD урсгалыг дотоод хязгаарлах SMS дэд бүтэц
		C76: Гүйлгээний хууль ёсны эсэхийг шалгахын тулд хоёр талын SecureOTP-г анхны утасны дугаар руу оруулна уу [7]
		C77: Мэдээллийг DFS үйлчилгээ үзүүлэгчийн сүлжээнд нэвтэрч, энэ орчинд боловсруулж, хадгалах үед нууцлал, бүрэн бүтэн байдлыг хангахын тулд хүчтэй криптографийн туршлагыг ашигла.
		C78: Хэрэглэгч бүрт DFS сессийн тоог хязгаарлах. Хандалтын сувгаас (STK, USSD, эсвэл https) үл хамааран хэрэглэгч бүрт нэг сесс хийхийг зөвшөөрөх; DFS хэрэглэгчийн бүртгэл нь олон сувгийг нэгэн зэрэг ашиглах боломжгүй байх ёстой.

(үргэлжлэл)

DFS үйлчилгээ үзүүлэгч		**C79:** Мобайл оператор нь SS7 халдлагын улмаас үүсэх аюулыг хязгаарлахын тулд GSMA-д (FS.11, FS.07, IR.82, IR.88) заасан SS7 болон диаметрийн дохиоллын аюулгүй байдлын хяналтыг байрлуулах ёстой.
	Хэрэглэгчийн нууц мэдээлэлд өртөх эрсдэл бий дараах эмзэг байдлаас болж.	
	- DFS хэрэглэгчийн бүртгэлийн мэдээллийн хамгаалалт хангалтгүй. (SD: Баталгаажуулалт)	**C80:** DFS бүртгэлд ашигладаг хэрэглэгчийн өгөгдлийг хамгаалах, хамгаалах, физик хэлбэрийг ашиглах, өгөгдлийг найдвартай хадгалах, дамжуулах.
	- Сул шифрлэлт ашиглах. (SD: Харилцаа холбооны аюулгүй байдал)	**C81:** API харилцааны хувьд TLS шифрлэлт v1.2 болон түүнээс дээш зэрэг хүчтэй шифрлэлтийн стандартыг ашиглана уу.

Нөлөөлөлд өртсөн аж ахуйн нэгж	**Эрсдэл ба эмзэг байдал**	**Хяналтууд**
DFS үйлчилгээ үзүүлэгч	- DFS хэрэглэгчийн хандалтын хяналт, хяналт хангалтгүй. (SD: Хандалтын хяналт)	**C82:** API-тай холбоотой аюул заналыг тодорхой тусгах зорилгоор аюул илрүүлэхийг өргөтгөх.
		C83: Алсын зайнаас нэвтрэх хандалтыг хязгаарлаж, арын DFS системд алсаас нэвтрэх сешнүүдийн эрхийг багасгах.
		C84: TLS гэрчилгээний ашиглалтын хугацааг 825 хоногоор хязгаарлах.
		C85: DFS системд холбогдсон бүх давуу эрхтэй хэрэглэгчид, агентууд болон худалдаачдын хэрэглэгчийн IP, төхөөрөмж болон нэвтрэх цагийг баталгаажуулна уу. Жишээлбэл, худалдаачин болон төлөөлөгчийн DFS системд хандах хандалтыг зөвхөн арилжааны нээлттэй цагаар ашиглах боломжтой байхаар тохируулаарай.
		C86: Үйлдвэрлэлийн платформ руу шилжихийн өмнө код болон өөрчлөлтийг туршилтын орчинд туршиж үзэх шаардлагатай; туршилтын орчин нь үйлдвэрлэлийн орчноос физик болон логикийн хувьд тусгаарлагдсан байх ёстой.
		C87: Аюулгүй байдлыг сайжруулахын тулд хэрэглэгчийн ПИН код, гүйлгээ, жетон, мөнгөний эрхийн бичгийг хамгаалахын тулд процессыг найдвартай удирдаж, криптограф түлхүүрүүдийг хадгалахын тулд Тоног төхөөрөмжийн аюулгүй байдлын модуль (HSM) гэх мэт хөндлөнгийн хамгаалалттай төхөөрөмжийг ашиглана уу.
		C88: Хамгийн бага давуу эрхийн зарчимд тулгуурлан хандалтын эрхийг тодорхойлохын тулд хэрэглэгчийн үүргийг тохируулна.
		C89: Хэрэглэгч, төлөөлөгч, худалдаачин, төлбөрийн үйлчилгээ үзүүлэгч эсвэл гуравдагч этгээдийн үйл ажиллагааг дуусгавар болгосны дараа холбогдох бүртгэлийг идэвхгүй болгох/идэвхгүй болгох
		C90: Бүртгэлийн зогсолтын хугацааг тогтоож, зогсолттой байгаа дансыг хугацаа дуусахад идэвхгүй болгоно.

(үргэлжлэл)

		C91: DFS-ийн үүрэг дээр үндэслэн нэвтрэх болон сессийн хязгаарлалтуудын хуваарийг тохируулах. (сессийн хязгаарлалт нь дүрд үндэслэн өдөрт хамгийн их буцаах тоог багтааж болно)
		C92: Хэрэглэгч нэмэх, өөрчлөх, устгах зэрэг DFS системд нэвтрэх эрхийг хязгаарлах, хянах, үе үе хянах.
		C93: API-ийн хэрэглээг хянах, гуравдагч этгээдтэй хуваалцсан бүх өгөгдлийг шифрлэх, мэдээлэл/мэдээлэл алдагдахаас зайлсхийхийн тулд төлбөрийн үйлчилгээ үзүүлэгчтэй байгуулсан нууцлалын гэрээ гэх мэт мэдээллийн удирдлагын журам, хяналтыг бий болгох.
	- Утасгүй сүлжээний хяналт хангалтгүй (SD: Мэдээллийн нууцлал)	**C94:** PCI DSS шаардлагын дагуу утасгүй дамжуулалтыг хамгаална. Хяналтад дараахь зүйлийг багтаах ёстой, гэхдээ үүгээр хязгаарлагдахгүй. - Худалдагчийн өгөгдмөл шифрлэлтийн түлхүүр, нууц үг болон SNMP нийгэмлэгийн мөрүүдийг өөрчилсөн эсэхийг шалгаарай. - Баталгаажуулах, дамжуулахад хүчтэй шифрлэлтийг хэрэгжүүлэхийн тулд салбарын шилдэг туршлагыг ашиглахад дэмжлэг үзүүлэх. - Интернэтэд холбогдсон сервер дээр тодорхой бичвэртэй дансны өгөгдөл хадгалагдахгүй байгаа эсэхийг шалгаарай.
Гуравдагч этгээд	- Төхөөрөмжийг устгахаас өмнө өгөгдлийг устгаж/арилгаж чадаагүй (SD: Нууцлал)	**C95:** DFS үйлчилгээ үзүүлэгчид **/** худалдаачид хуучин төхөөрөмжүүдийг тогтмол устгаж байх ёстой. Шийдэл нийлүүлэгч зааварчилгаа өгөх үед худалдаачин үүнийг дагаж мөрдөх ёстой. Зарим зүйлийг анхаарч үзэх хэрэгтэй: - Бүх шошго болон бизнесийн таниглийг устгана уу. - Боломжтой бол цахим материал, эд ангиудыг найдвартай устгахад туслах эрх бүхий борлуулагчтай гэрээ байгуул. - Танай бизнестэй холбоотой төхөөрөмжийг хогийн сав, хогийн саванд бүү хая.

8.13. Аюул: Хортой програм

Бид энэхүү ерөнхий аюулыг DFS доторх элементүүд нь хортой програмаар халдварлахад өртөмтгий гэж тодорхойлдог.

Нөлөөлөлд өртсөн аж ахуйн нэгж	Эрсдэл ба эмзэг байдал	Хяналтууд
Гуравдагч этгээд, DFS үйлчилгээ үзүүлэгч	**Хортой програмын халдлага, гүйлгээ хийх боломжгүй, үйлчилгээний тасалдал, өгөгдөлд зөвшөөрөлгүй хандалт** зэргээс шалтгаалсан эрсдэлүүд нь дараах эмзэг байдлын улмаас Худалдаачин / DFS үйлчилгээ үзүүлэгч дээр үүсдэг.	
	- Хортой програм эсвэл вирусын эрсэг програм хангамжийг ашиглаагүй тохиолдолд байнга шинэчлэгддэг эсвэл байнга шинэчлэгддэг (SD: Боломжтой)	**C96:** Вирусны эрсэг, тагнуулын эрсэг программ хангамж, програм хангамжийн баталгаажуулалтын бүтээгдэхүүн зэрэг бүх хөдөлгөөнт төхөөрөмж дээр аюулгүй байдлын програм хангамжийн бүтээгдэхүүнийг байрлуулж, системийг одоогийн болон хөгжиж буй хортой програм хангамжийн аюулаас хамгаалах. Бүх програм хангамжийг найдвартай эх сурвалжаас суулгасан байх ёстой.
		C97: Хортой программ хангамжийн эсрэг програм хангамж байхгүй бол төхөөрөмжөөс хортой программ хангамж болон програмуудыг хянах, үнэлэх, устгах боломжтой MAM (Мобайл хэрэглээний менежмент) эсвэл MDM шийдлүүдийг ашигла. Цаашилбал, хэрэв боломжтой бол төхөөрөмжийг хортой программ хангамж, програмаас хамгаалахын тулд вирусын эсрэг болон MDM шийдлүүдийг (дээр дурдсан) хоёуланг нь ашиглах нь хамгийн тохиромжтой.
		C98: Төхөөрөмжийн шаардлагагүй функцуудыг идэвхгүй болгож, зөвхөн баталгаажсан програм хангамжийг суулгана уу Худалдаачид болон DFS үйлчилгээ үзүүлэгчид төлбөрийн шийдлийн үйл ажиллагаанд шаардлагагүй аливаа харилцааны чадамжийг идэвхгүй болгох ёстой. Хөдөлгөөнт төхөөрөмжид халдлагын шинэ векторуудыг нэвтрүүлэхээс зайлсхийхийн тулд зөвхөн бизнесийн үйл ажиллагааг дэмжих, төлбөрийг хөнгөвчлөхөд шаардлагатай баталгаажсан программ хангамжтай холбогдохыг зөвшөөрнө үү.
	- Худалдан авсан гар утасны төхөөрөмжийн аюулгүй байдлын талаар шийдэл нийлүүлэгчтэй хангалтгүй хамтын ажиллагаа (SD: Олдоц ба нууцлал)	**C99:** Худалдаачид болон DFS үйлчилгээ үзүүлэгчид шийдэл нийлүүлэгчээсээ дараахь зүйлийг шаардах ёстой. - Шийдэл нийлүүлэгч нь төлбөрийн програмаа тогтмол шинэчилж, шинэчлэлтүүд бэлэн байгаа бөгөөд суулгахад аюулгүй гэдгийг худалдаачдад зааж өгөх ёстой. - Шийдэл нийлүүлэгч нь төлбөрийн програмдаа хязгаарлалттай байх ёстой бөгөөд энэ нь зөвхөн батлагдсан програм хангамжийг ажиллуулж байгаа төхөөрөмж дээр ажиллах болно. - Шийдэл нийлүүлэгч нь худалдаачны дагаж мөрдөх шаардлагатай шинэчлэлтийн журмыг нарийвчлан харуулсан баримт бичгийг нийлүүлэх ёстой. - DFS шийдлийн үйлчилгээ үзүүлэгч нь DFS үйлчилгээ үзүүлэгчтэй холбогдож, төлбөр хүлээн авах шийдэлд шинээр илэрсэн сул талуудын талаар тэдэнд мэдэгдэх ёстой. Нэмж дурдахад, шийдлийн үйлчилгээ үзүүлэгч нь шинэ эмзэг байдал илэрсэн үед худалдаачдыг удирдан чиглүүлэхээс гадна эдгээр эмзэг байдлын аль нэгийг шалгасан засваруудыг өгөх ёстой.

(үргэлжлэл)

	- Илрүүлээгүй системийн програмын сул талуудыг нээх (SD: Мэдээллийн нууцлал)	**C100:** Худалдаач нь аливаа аудит эсвэл бүртгэл хөтлөх чадварыг идэвхжүүлэхийн тулд шийдэл нийлүүлэгчтэйгээ хамтран ажиллах ёстой. Шийдэл нийлүүлэгч нь хэвийн бус үйл явдлуудыг илрүүлэх хангалттай нарийвчлалтайгаар бүртгэл хөтлөх чадвартай эсэхийг баталгаажуулах ёстой. Шийдэл нийлүүлэгч нь бүртгэлийг шалгахын тулд худалдаачны хариуцлагын талаар худалдаачинд чиглүүлэх ёстой. Нэмж дурдахад системийн бүртгэл, тайланг хэвийн бус үйл ажиллагаатай эсэхийг тогтмол шалгана. Хэрэв хэвийн бус үйл ажиллагаа сэжиглэгдсэн эсвэл илэрсэн бол асуудлыг шийдэж дуустал мобайл төхөөрөмж болон түүний төлбөрийн аппликейшнд хандахыг зогсооно уу. Хэвийн бус үйлдлүүд нь зөвшөөрөлгүй нэвтрэх оролдлого, өргөжүүлсэн эрх, программ хангамж эсвэл програм хангамжийн зөвшөөрөлгүй шинэчлэлтүүд орно, гэхдээ үүгээр хязгаарлагдахгүй.
Гуравдагч этгээд, DFS үйлчилгээ үзүүлэгч	- Сүлжээнд гадны халдлагад өртөх (SD: Боломж)	**C101:** DFS програмууд нь аюулгүй байдлын нэвтрэлтийн сканнер болон нэвтрэлтийн шалгалтанд тогтмол хамрагдах ёстой. Ялангуяа программууд нь фишинг программ хангамжийн эсрэг бат бөх байхаар бүтээгдсэн байх ёстой.
	Тагнуулын програм, троян зэрэг хортой програм суулгах эрсдэл тохиолддог дараах эмзэг байдлын улмаас: - Хортой программ эсвэл вирусын эсрэг программ ашигладаггүй, байнга шинэчлэгддэггүй (SD: Боломжтой байдал)	**C102:** Хөдөлгөөнт төхөөрөмжийн үйлдлийн системийг тогтмол шинэчилж байх; хэрэглэгчийн баталгаажуулалтгүйгээр програм суулгахыг бүү зөвшөөр.
	Алсын зайнаас код гүйцэтгэх эрсдэл нь дараахь эмзэг байдлаас шалтгаална.	
Гар утасны хэрэглэгч	- Хуучирсан төхөөрөмжийн програм хангамж (SD: Мэдээллийн нууцлал)	**C103:** Мобайл хэрэглэгчид DFS гүйлгээнд ашигладаг мобайл төхөөрөмждөө аюулгүй байдлын шинэчлэлтүүдийг тогтмол хийж, төхөөрөмж үйлдвэрлэгчид болон програм хангамжийн үйлчилгээ үзүүлэгчдийн хамгийн сүүлийн үеийн аюулгүй байдлын засваруудаар шинэчлэгдэж байхыг дэмжих хэрэгтэй.
	- Хортой программ эсвэл вирусын эсрэг программ ашигладаггүй, байнга шинэчлэгддэггүй (SD: Боломжтой байдал)	**C104:** Вирусны эсрэг, тагнуулын эсрэг программ болон программ хангамжийн баталгаажуулалтын бүтээгдэхүүн зэрэг найдвартай эх сурвалжаас аюулгүй байдлын программ хангамжийг мобайл төхөөрөмж дээр суулгаж, төхөөрөмжийг одоо байгаа болон хөгжиж буй хортой програмын аюулаас хамгаалах болно.
	- Хэрэглэгчийн төхөөрөмжийг өөрчлөх, үндэслэх (SD: Integrity)	**C105:** Учир нь хөндлөнгийн оролцоотой буюу "үндэс" төхөөрөмж нь хэрэглэгчийн мэдээллийн нууцлал, бүрэн бүтэн байдал, нууцлалыг алдагдуулж болзошгүй.
		C106: Мобайл програм хөгжүүлэгч нь DFS програмуудыг хамгаалагдсан байх ёстой бөгөөд ингэснээр хөдөлгөөнт төхөөрөмж дээрх бусад найдвартүй програмууд нь DFS програмтай харьцах боломжгүй, үйлдлийн системтэй харилцах нь хязгаарлагдмал байх ёстой.
MNO	**Гүйлгээ хийх чадваргүй болох, үйлчилгээнд буулт хийх** эрсдэл нь дараахь эмзэг байдлын улмаас үүсдэг. - Сүлжээнд гадны халдлагад өртөх (SD: Боломж)	**C107:** Системийн хүртээмжид нөлөөлж болзошгүй халдлагад өртөх эсэхийг шалгахын тулд MNO дэд бүтцийн эмзэг байдлын сканнер болон нэвтрэлтийн тестийг тогтмол хийнэ.
		C108: Хамгийн сүүлийн үеийн вирусын эсрэг программ хангамжийг (хэрэв байгаа бол) суулгаж, тогтмол шинэчилж, үүнийг эцсийн хэрэглэгчид ашиглах боломжтой болго. Хортой программ хангамж, программаас урьдчилан сэргийлэх, устгахын тулд MDM (Мобайл төхөөрөмжийн менежмент) шийдлүүдийн хамт ашиглаж болох програмын багцыг авч үзье.

8.14. Аюул: Тэг халдлага

Хортой программаас хамгаалах уламжлалт арга хэрэгсэл нь урьд өмнө тохиолдож байгаагүй аюулын эсрэг үр дүнгүй байдаг тул бид хортой програмын аюулын энэ дэд бүлгийг авч үздэг.

8.15. Аюул: Хуурамч төхөөрөмжүүд

Бид DFS сүлжээний дэд бүтцэд зөвшөөрөлгүй төхөөрөмж үзүүлж болзошгүй аюулыг авч үздэг.

Нөлөөлөлд өртсөн аж ахуйн нэгж	Эрсдэл ба эмзэг байдал	Хяналтууд
MNO	**Залилан мэхлэх, өгөгдлийг өөрчлөх** эрсдэл дараах эмзэг байдлын улмаас үүсдэг - DFS дэд бүтцэд холбогдсон хамгаалалтгүй төхөөрөмжүүд (SD: Өгөгдлийн бүрэн бүтэн байдал)	**C111:** MNO нь DFS системд холбогдох эсвэл өөр аргаар хандахад ашигладаг төхөөрөмжүүдийг хянаж байх ёстой бөгөөд эдгээр төхөөрөмжүүд нь хамгийн сүүлийн үеийн засварууд, шинэчлэгдсэн вирусын эсрэг программ хангамж, rootkit болон түлхүүр бүртгэгчид сканнердсан, сүлжээ өргөтгөгчийг дэмждэггүй эсэхийг шалгах ёстой.

8.16. Аюул: Мобайл төхөөрөмжид зөвшөөрөлгүй нэвтрэх

Энэхүү аюул заналхийлэл нь халдагчдын гар утасны төхөөрөмжүүдийн эсрэг түсгай халдлага гэж тодорхойлогддог.

Нөлөөлөлд өртсөн аж ахуйн нэгж	Эрсдэл ба эмзэг байдал	Хяналтууд
Гар утасны хэрэглэгч/төхөөрөмж	**Хуурамчлах, мэдээлэл алдах/хууран мэхлэх гүйлгээний** эрсдэл дараах эмзэг байдлын улмаас үүсдэг.	
	- Төхөөрөмж дээрх хэрэглэгчийн баталгаажуулалт хангалтгүй (SD: Мэдээллийн нууцлал)	**C112:** Хөдөлгөөнгүй төхөөрөмжүүд хэсэг хугацаанд идэвхгүй болсны дараа автоматаар түгжигдэх ёстой бөгөөд энэ нь DFS гүйлгээнд ашиглахаас өмнө төхөөрөмжийн түгжээг тайлахын тулд төхөөрөмжийн нэвтрэлт танилтыг хийх шаардлагатай болдог.
		C113: Төхөөрөмжийн ийм боломжууд байгаа үед хүчтэй PIN код ашиглах, өгөгдлийг алсаас устгах, PIN түгжих, биометрийн баталгаажуулалтыг (жишээ нь, хурууны хээ, цахилдаг) ашиглана уу.
	- Хэрэглээний програм хангамжийн хүүчирсан хувилбарууд нь төхөөрөмжийг хортой програмд өртөмтгий болгодог (SD: Мэдээллийн нууцлал	**C114:** Төхөөрөмжийн үйлдвэрлэгчид чухал шинэчлэлтүүдийг хэрэглэгчдэд шууд авах эсвэл сүлжээнд ашиглах боломжтой болгохыг баталгаажуулах ёстой.
DFS үйлчилгээ үзүүлэгч	*DFS* **хэрэглэгчийн бүртгэлийг бүлаан авах** эрсдэл нь дараах эмзэг байдлын улмаас үүсдэг. - DFS дэд бүтцэд хэт зөвшөөрөгдсөн хандалт (SD: Баталгаажуулалт)	**C115:** DFS хэрэглэгчдийг баталгаажуулахын өмнө боломжтой бол хэрэглэгчийн IMSI, төхөөрөмж, байршил, IP хаягийг баталгаажуулж, сүлжээний дэд бүтцэд зөвшөөрөлгүй нэвтрэхээс сэргийлж, тэдний таних тэмдэгийг тогтооно.
Гуравдагч этгээдийн үйлчилгээ үзүүлэгч	**Татгалзсан гүйлгээний** эрсдэл нь дараахь эмзэг байдлын улмаас үүсдэг. - Гүйлгээний баталгаажуулалт хангалтгүй (SD: Татгалзахгүй)	**C116:** Төлбөрийн үйлчилгээ үзүүлэгч нь DFS данстай холбогдсон ерөнхий зориулалтын дахин цэнэглэх боломжтой картууд нь ПИН код эсвэл биометр зэрэг карт эзэмшигчийн баталгаажуулалтын арга бүхий EMV чип ашиглахыг шаардлагатай бол бүх гүйлгээний үр дүнд харилцагчдад анхааруулга өгөх ёстой.

Нөлөөлөлд өртсөн аж ахуйн нэгж	Эрсдэл ба эмзэг байдал	Хяналтууд
MNO, DFS үйлчилгээ үзүүлэгчид болон гуравдагч этгээдүүд	**Хэрэглэгчийн нууц мэдээлэлд зөвшөөрөлгүй хандах, хэрэглэгчийн мэдээлэлд зөвшөөрөлгүй өөрчлөлт оруулах** эрсдэл нь дараахь эмзэг байдлын улмаас үүсдэг. - Байршуулсан системийн эсрэг шинэ мөлжлөгүүдийг илрүүлэх, эдгээр мөлжлөгийн эсрэг шийдлийг ашиглах боломжгүй байх (SD: Өгөгдлийн нууцлал, хандалтын хяналт, хүртээмж)	**C109:** MNO-ууд DFS үйлчилгээ үзүүлэгч болон төлбөрийн үйлчилгээ үзүүлэгчдийн хамт хуучин эмзэг байдлаас үүссэн халдлагаас хамгаалахын тулд борлуулагчаас өгсөн хамгийн сүүлийн үеийн хувилбарт системийг нөхөх ёстой. **C110:** Зэрлэг байгальд тэг өдрийн халдлага илэрсэн тохиолдолд үйлчилгээ үзүүлэгч болон МҮО-ууд засвар үйлчилгээ хийх, системийн засварыг хурдан шуурхай авахын тулд борлуулагчидтай хамтран гэнэтийн төлөвлөгөөтэй байх ёстой. Энэхүү стратегийн нэг хэсэг нь нөөцлөлтийг зөв ашиглах явдал юм.

(үргэлжлэл)

8.17. Аюул: Хувийн мэдээллийг санамсаргүй задруулах

Бид энэ олон аюулыг хэрэглэгчийн мэдээлэл санамсаргүйгээр ил гаргахад хүргэдэг гэж тодорхойлдог.

Нөлөөлөлд өртсөн аж ахуйн нэгж	**Эрсдэл ба эмзэг байдал**	**Хяналтууд**
DFS үйлчилгээ үзүүлэгч	**Хувь хүний тодорхойлох мэдээлэлд өртөх** эрсдэл дараах эмзэг байдлын улмаас үүсдэг. - Туршилтын орчин дахь хяналт, хяналт хангалтгүй (SD: нууцлал)	**C117:** DFS үйлчилгээ үзүүлэгчид шилдэг туршлагын дагуу нэрээ нууцлахаас бусад тохиолдолд үйлдвэрлэлийн орчин дахь хэрэглэгчийн өгөгдлийг туршилтын орчинд ашиглахгүй байхыг баталгаажуулах ёстой. Үүний эсрэгээр, туршилтын өгөгдлийг бүтээгдэхүүн рүү шилжүүлж болохгүй.
Нөлөөлөлд өртсөн аж ахуйн нэгж	**Эрсдэл ба эмзэг байдал**	**Хяналтууд**
Гуравдагч этгээдийн үйлчилгээ үзүүлэгч	**Нууц мэдээлэлд өртөх** эрсдэл дараах эмзэг байдлын улмаас үүсдэг.	
	- Хэрэглэгчийн мэдрэмтгий мэдээллийг гүйлгээ эсвэл API-ээр дамжуулан ил гаргах (SD: нууцлал)	**C118:** Гуравдагч талын үйлчилгээ үзүүлэгчид төлбөрийн үйлчилгээ үзүүлэгч болон DFS үйлчилгээ үзүүлэгч зэрэг бусад талуудтай мэдээлэл хуваалцахыг гүйлгээний бүрэн бүтэн байдлыг хангахад шаардагдах хамгийн бага хэмжээнд хязгаарлах ёстой.
	- Өгөгдлийн хамгаалалтын хяналт хангалтгүй (SD: нууцлал)	**C119:** Үйлчилгээ үзүүлэгч нар хэрэглэгчийн мэдрэмтгий өгөгдлийг ул мөрийн бүртгэл (жишээлбэл, бэлэн мөнгө авах эрхийн бичгийн код, банкны дансны дугаар, баталгаажуулалт) зэрэг орчноос устгасан байх ёстой. Бүртгэлийн файлд энэ өгөгдлийг харуулахын тулд боломжтой бол газар эзэмшигчийг ашиглана уу.

9. ХЭРЭГЛЭЭНИЙ АЮУЛГҮЙ БАЙДЛЫН ШИЛДЭГ ТУРШЛАГЫН ЗАГВАР

Энэ хэсэгт бид цахим мөнгө, ухаалаг гар утасны хэрэглээний аюулгүй байдлын хүрээий загварыг авч үзэх болно. Энд гол анхаарал хандуулсан зүйл бол ерөнхий шилдэг туршлагууд бөгөөд тодорхой хэлэлцсэнээс бусад тохиолдолд тусгай технологид биш юм.

Энэхүү загварын хувьд бид мобайл, цахим мөнгөний аппликейшний аюулгүй байдлын шилдэг туршлагын талаарх GSMA судалгаа, [9] ENISA ухаалаг гар утсыг аюулгүй хөгжүүлэх удирдамж, [10] , гар утасны төлбөр зэрэг дижитал санхүүгийн үйлчилгээний програмуудыг мобайл мөнгөний хэрэглээний талбар талаас нь судлах сүүлийн үеийн ажлуудад тулгуурласан болно. Пакистаны Төрийн банкнаас боловсруулсан програмуудын аюулгүй байдлын хүрээ. [11] Энэ загварыг мөн DFS үйлчилгээ үзүүлэгчдийн програмын аюулгүй байдлын бодлогын ролт болгон ашиглаж болно.

Энэ хэсэгт бид зохицуулагчид эсвэл хэрэглээний аюулгүй байдлын шалгагчдад аюулгүй байдлын үнэлгээ хийх эхлэлийн цэг болгон зөвлөмжүүдийг нэгтгэн харуулав. Загвар нь өөрөөр заагаагүй бол төхөөрөмж дээрх гар утасны програмыг нарийн авч үздэг бөгөөд зөвлөмжийг тайлбарласан дэд хэсгүүд нь үйл ажиллагааны янз бүрийн асуудал эсвэл гар утасны програмтай холбоотой үндсэн бодлогыг авч үздэг. Гар утасны үйлдлийн системд олон зөвлөмжийг ашиглах боломжтой хэдий ч зах зээлд эзлэх хувь хэмжээ нь үндсэндээ Android програмууд дээр төвлөрдөг. Нууцлал нь бас анхаарах ёстой чухал хүчин зүйл боловч эдгээр зөвлөмжүүд нь аюулгүй байдалд анхаарлаа хандуулдаг.

9.1. Төхөөрөмж ба хэрэглээний бүрэн бүтэн байдал

i. Санхүүгийн гүйлгээг хийхэд хамгийн найдвартай төхөөрөмжүүд нь “jailbreak” буюу “rooted” хийгээгүй төхөөрөмжүүд юм. Тиймээс програмууд нь гар утасны платформын үйлчилгээг ашиглан өөрт болон үндсэн платформ нь өөрчлөгдөөгүй гэдгийг тодорхойлох ёстой.

ii. Аппликешныг ашиглах гэж буй төхөөрөмжийн платформд зориулагдаагүй функцууд эсвэл байршуулсан үйлдвэрлэлийн кодын халдлагыг багасгахын тулд хөгжүүлэгч/дибаг хийх функцууд гэх мэт хөгжүүлэлтийн явцад програмд нэмэгдсэн байж болзошгүй аливаа нэмэлт кодыг устгана уу.

iii. Сервер талд гарын үсгийн баталгаажуулалт эсвэл програм эсвэл тодорхой програмын функцийн блокууд дээр хэш хийх замаар програм нь бүрэн бүтэн байдалд ажиллаж байгаа эсэхийг тодорхойлно.

9.2. Харилцаа холбооны аюулгүй байдал ба гэрчилгээтэй ажиллах

I. Аппликешн нь стандартчилсан криптографийн санг ашиглаж, арын үйлчилгээтэй харилцахдаа стандартчилсан протокол, ялангуяа TLS бүхий төгсгөлөөс төгсгөлд шифрлэлтийг ашиглах ёстой. TLS-ийн хамгийн бага санал болгосон хувилбар нь 1.2 хувилбар юм. ii. TLS гэрчилгээний хугацаа дуусаагүй байх ёстой бөгөөд хүчтэй шифрийн багц, ялангуяа AES-128 шифрлэлт болон хэш хийх SHA-256 байх ёстой. GCM гэх мэт баталгаажсан шифрлэлтийн горимуудыг дэмждэг.

II. CA/Browser Forum шилдэг туршлагын дагуу олгосон гэрчилгээний ашиглалтын хугацааг 825 хоногоор хязгаарлана.

III. Гэрчилгээний байгууллагын найдвартай байдлыг баталгаажуулж, хэрэв CA-д итгэхээ больсон тохиолдолд урьдчилан сэргийлэх төлөвлөгөөг анхаарч үзээрэй.

IV. TLS-ийн тохиргоог найдвартай хийж байгаа эсэхийг баталгаажуулж, баталгаажуулалт хийхгүй байх эсвэл алгоритмын бруу сонголтод хүргэж болзошгүй бруу тохируулгын асуудлаас зайлсхий. vi. Сертификатыг солихоос урьдчилан сэргийлэхийн тулд гэрчилгээг бэхлэхийг зөвлөж байна.

V. Үйлчлүүлэгч төхөөрөмжүүд нь зөв ажиллаж байгаа эсэхийг баталгаажуулах ёстой. DATE серверийн гэрчилгээ.

9.3. Хэрэглэгчийн баталгаажуулалт

I. ПИН код болон нууц үгийг таахад хялбар байх ёсгүй бөгөөд сул баталгаажуулалтыг зөвшөөрөхгүй байх; Гэсэн хэдий ч хэрэглэгчид нууц үгээ байнга солихыг албадах ёсгүй.

II. Санхүүгийн болон бусад эмзэг функцийг гүйцэтгэхийн өмнө олон хүчин зүйлийн баталгаажуулалтыг дэмждэг.

III. SS7 хулгайлах болон бусад аюулгүй байдлын улмаас SMS илгээхээс илүүтэй нэг удаагийн нууц үг илгээхэд ухаалаг утасны баталгаажуулагч програмуудыг ашиглах хэрэгтэй. iv. Хэрэв биометрийн мэдээллийг баталгаажуулалтад ашиглаж байгаа бол үүнийг Android түлхүүрийн дэлгүүрт шифрлэгдсэн эсвэл найдвартай техник хангамж ашиглах зэрэг аюулгүй байдлын зохих арга хэмжээнүүдийн дагуу хадгалах ёстой.

9.4. Мэдээллийн аюулгүй ажиллагаа

i. Мобайл төхөөрөмж нь нууц мэдээллийг, жишээлбэл, Android KeyStore хүрээг ашиглан найдвартай хадгалах ёстой.

ii. Баталгаажсан техник хангамжийг үйлчлүүлэгчийн ухаалаг утсанд ашиглах боломжтой бол нууц мэдээллийг хадгалахад ашиглах ёстой.

iii. Мэдээллийг гадаад санах ойд хадгалахаас зайлсхийж, хэрэв үүнийг хийсэн бол энэ өгөгдлийг ашиглахаас өмнө хүчтэй оролтын баталгаажуулалт хийсэн эсэхийг шалгаарай. iv. Нууц өгөгдлийг ашигласны дараа кэш болон санах ойноос устгаж, мэдээлэлд ерөнхий өртөхөөс зайлсхийх (жишээ нь, нууц түлхүүрийг стек дээр байрлуулах). Програмаас гарахын өмнө санах ойг цэвэрлэж байгаарай.

v. Нарийн зөвшөөрлөөр дамжуулан бусад програмуудтай хуваалцсан өгөгдлийг хязгаарлах. Апп-аас хүссэн зөвшөөрлийн тоог багасгаж, зөвшөөрөл нь программыг ажиллуулахад шаардлагатай функцтэй хамааралтай эсэхийг шалгаарай.

vi. Нууц үг, түлхүүр гэх мэт эмзэг мэдээллийг програмын эх код руу бүү хатуу кодчил.

vii. SQL тарилгын халдлагаас зайлсхийхийн тулд өгөгдлийн санд хадгалагдах үйлчлүүлэгчээс ирсэн аливаа оролтыг баталгаажуулна уу.

9.5. Аюулгүй програм хөгжүүлэлт

i. Салбарт хүлээн зөвшөөрөгдсөн аюулгүй кодчилол, стандартын дагуу программуудыг хөгжүүлэх.

ii. Аппликешнүүдийг найдвартай шинэчлэх арга хэрэгслийг баталгаажуулж, бүх хамааралтай номын сан, модулиудыг найдвартай байлгах; шаардлагатай үед эдгээрийн шинэчлэлтүүдийг өгөх.

iii. Кодыг дотоод болон гадаад кодын хянан шалгах багууд бие даан үнэлж, туршиж үзээрэй.

10. DFS-ийн АЮУЛГҮЙ БАЙДЛЫН ҮЙЛ АЖИЛЛАГААНЫ МЕНЕЖМЕНТ

Холбогдох хяналтыг хэрэгжүүлсний дараа ч, халдагчид системээс зайлсхийх санхүүгийн зорилготой байдаг санхүүгийн үйлчилгээнүүдэд энэ нь системийн тасалдал, өгөгдлийг өөрчлөх, задруулахад хүргэдэг. Санхүүгийн дижитал үйлчилгээг санал болгож, үүнд оролцдог байгууллага, оролцогч талууд аюулгүй байдлын зөрчлийг амжилттай ойлгох, удирдах, сэргээх боломжийг олгох зөв журам, тайлагнах, мэдээлэл цуглуулах, удирдлагын хариуцлага, хууль эрх зүйн протокол, харилцааны стратегийг боловсруулах шаардлагатай.

Ослын менежментийн төлөвлөгөөгүй DFS үйлчилгээ үзүүлэгч нь халдлагыг эхний ээлжинд илрүүлж чадахгүй, эсвэл хэрэв халдлага илэрсэн бол үйлчилгээ үзүүлэгч нь гэмтлийг хурдан арилгах, халдагчийн үүсэгсэн нөхцлөл байдлыг арилгах, хариу арга хэмжээ авах, түүнийг сэргээх журамгүй байна гэсэн үг юм.

Аюулгүй байдлын ослын менежментийн төлөвлөгөө нь аюулгүй байдлын найман хэмжүүрийн аль нэгийг нь зөрчиж буй аюулгүй байдлын зөрчлүүдийг эмх цэгцтэй, хурдан бөгөөд үр дүнтэй мэдээлэх, хариу арга хэмжээний дүн шинжилгээ хийх, мөрдөн шалгах, сэргээхэд баримтлах журмыг тодорхойлдог.

ISO/IEC 27035:2016 Мэдээллийн аюулгүй байдлын ослын менежмент нь мэдээллийн аюулгүй байдлын хяналт нь төгс бус бөгөөд ослыг зохицуулах нарийвчилсан үйл явцтай гэдгийг хүлээн зөвшөөрдөг.

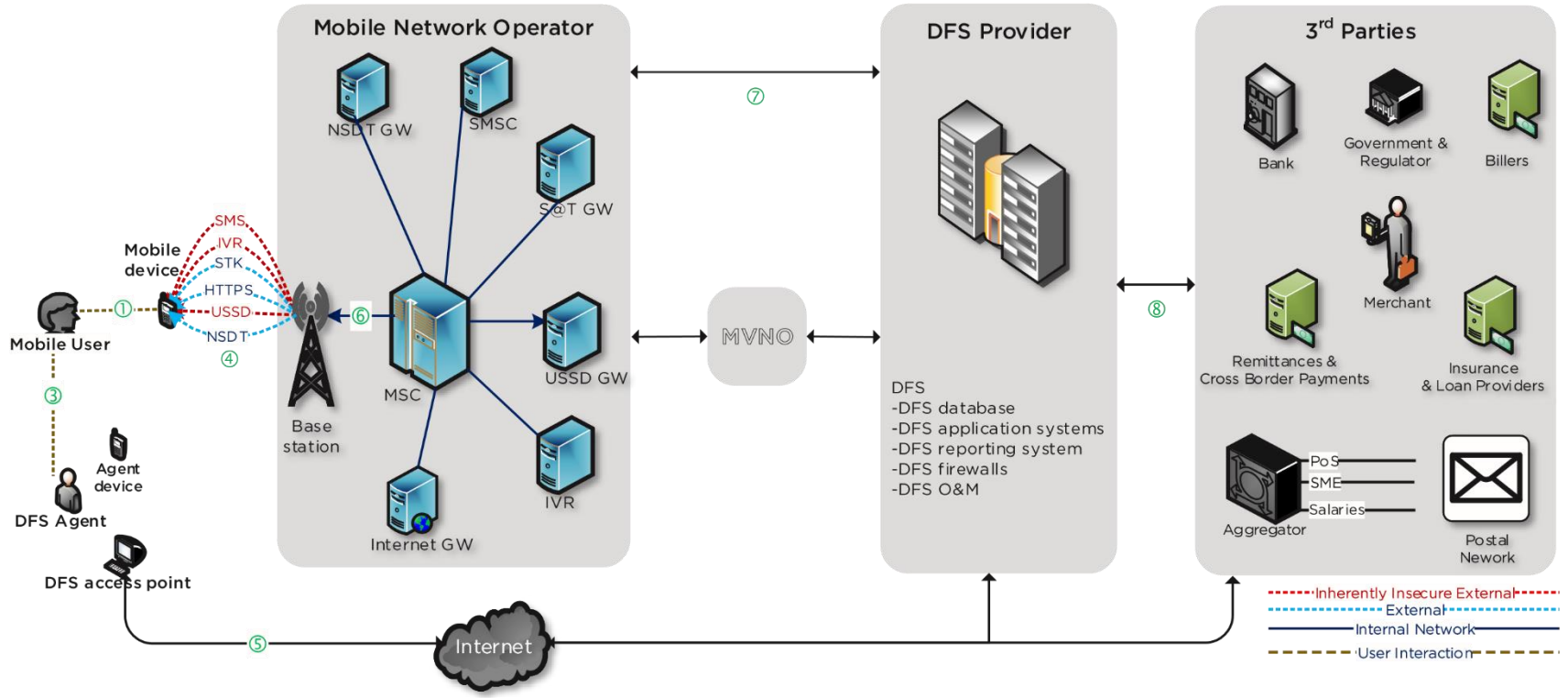
Интернэтийн аюулгүй байдлын төв [12] нь ослын менежментийн талаар DFS системийн сүлжээний операторууд, DFS үйлчилгээ үзүүлэгчид болон үйлчилгээ үзүүлэгчдийн хэрэглэж болох дараах удирдамжийг санал болгож байна.

1. Ажилтны үүрэг, ослыг зохицуулах/удирдах үе шатуудыг тодорхойлсон ослын хариу арга хэмжээний төлөвлөгөөг бичгээр гаргасан эсэхийг баталгаажуулах.
2. Компьютер, сүлжээний ослыг шийдвэрлэх ажлын байрны нэр, үүрэг хариуцлагыг тодорхой хүмүүст хуваарилж, шийдвэрлэх замаар ослыг хянах, баримтжуулах.
3. Удирдлагын боловсон хүчин, түүнчлэн шийдвэр гаргах гол үүрэг гүйцэтгэх замаар ослыг шийдвэрлэх үйл явцыг дэмжих нөөц хүмүүсийг томилох.
4. Системийн администраторууд болон бусад ажиллах хүчний гишүүдийн осолтой харьцах багт хэвийн бус үйл явдлыг мэдээлэхэд шаардагдах хугацаа, ийм мэдээлэх механизм, ослын мэдэгдэлд тусгах ёстой мэдээллийн төрлөөр байгууллагын хэмжээнд стандарт боловсруулах.
5. Хууль сахиулах байгууллага, төрийн холбогдох хэлтэс, худалдагч, төхөөрөмж үйлдвэрлэгч зэрэг аюулгүй байдлын зөрчлийн талаар мэдээлэхэд ашиглах гуравдагч этгээдийн холбоо барих мэдээллийн мэдээллийг цуглуулж, хадгалах.
6. Компьютерийн гажиг, ослын талаар мэдээлэхтэй холбоотой бүх ажиллах хүчний гишүүдэд зориулсан мэдээллийг ослыг шийдвэрлэх багт нийтлэх. Ийм мэдээллийг ажилчдыг сурталчлах ердийн үйл ажиллагаанд оруулах.
7. Бодит ертөнцийн аюул заналхийлэлд хариу үйлдэл үзүүлэхэд ухамсар, тав тухтай байдлыг хадгалахын тулд ослын хариу арга хэмжээнд оролцож буй ажиллах хүчний хувьд ослын хариу арга хэмжээний ердийн дасгал, хувилбаруудыг төлөвлөж, явуул. Дасгал нь харилцааны суваг, шийдвэр гаргах, осолд хариулагчийн техникийн чадавхийг тэдэнд байгаа багаж хэрэгсэл, өгөгдлийг ашиглан шалгах.
8. Байгууллагадаа мэдэгдэж байгаа эсвэл болзошгүй нөлөөлөл дээр үндэслэн ослын оноо, эрэмбэлэх схемийг үүсгэ. Статус шинэчлэлтийн давтамж болон эрчимжүүлэх процедурыг тодорхойлохын тулд онооны схемийг ашиглах.

Annex 1 Detailed DFS ecosystem infrastructure and threats

There are many interaction points between different parties within the DFS. Consequently, there are also a number of ways in which attackers can leverage these interfaces to attack the system, with successful exploits often having consequences that affect not merely the exploited stakeholders but others within the ecosystem. We consider the detailed diagram below showing the different vulnerable points in the DFS infrastructure in this section. The numbers will be used as a means of describing the vulnerability surface that occurs at that interaction point.

Figure 14 - Mapping of threats to security controls



1. үйлчлүүлэгч - хөдөлгөөнт төхөөрөмж

a. Хэрэглэгч төхөөрөмжөө бусадтай хуваалцсан, гээгдүүлсэн, хулгайлсан, хураан авсан, эсхүл өрсөлдөгчид хэрэглэгчийн баталгаажсан аялж байснаас болж хэрэглэгчийн эмзэг мэдээлэл ил болсон.

b. дээрх PIN код эсвэл нууц үгийг тааварласан халдагчид төхөөрөмжид зөвшөөрөлгүй нэвтрэх эсвэл таних механизмыг (хэрэв тохируулсан бол) өөр аргаар устгасан.

c. Үндсэн платформын аюулгүй байдлыг алдагдуулахын тулд төхөөрөмжид хөндлөнгөөс оролцох, тухайлбал, үндсэн санах ойд хортой програм суулгах эсвэл төхөөрөмжийн санах ойноос нууцыг задлах.

d. Дүүдлага болон SMS дамжуулалтыг тохируулахын тулд зөвшөөрөлгүй хорлонтой халдагч дүүдлагын тохиргоог өөрчилснөөр халдагчид OTP гэх мэт мессежээр илгээсэн DFS мэдээлэлд хандах боломжтой болно.

2. Мобайл төхөөрөмж - гар утасны програм

a. Хөдөлгөөнт хэрэглүүр доторх кодын эмзэг байдлыг халдагчид гар утасны төхөөрөмжид, тухайлбал, хэт их хэрэглүүрээр дамжуулан ашиглаж болно. Энэ нь хэрэглэгчийн мэдээлэл алдагдах, нууцлал алдагдах, бүрэн бүтэн байдал алдагдах зэрэгт хүргэж болзошгүй.

b. Үндсэн мобайл платформыг эвдэх нь вирус, троян, ransomware болон бусад хортой програм/rootkit-үүдыг нэвтрүүлж, хэрэглэгчийн мэдээллийг алдах, эсвэл хэрэглэгчийг програмын баталгаажуулалтыг олж авах гэсэн фишинг оролдлогод өртөмтгий болгож, халдагчдад боломж олгох боломжтой. хэрэглэгчийн данс руу зөвшөөрөлгүй нэвтрэх.

c. Аппликешн доторх хандалтын хяналт хангалтгүй,

Жишээ нь, итгэлцлийн талаарх таамаглалд тулгуурласан эмзэг үйлдлүүд (жишээ нь, бүртгэл, төлбөрийн шилжүүлэг) хийхээс өмнө шаардлагатай баталгаажуулалтын механизм нь хэрэглэгчийн мэдээллийг задруулж, улмаар зөвшөөрөлгүй мөнгө шилжүүлэхэд хүргэдэг.

d. Аппликешн дотор бүртгэл хийх/аудит хийх чадвар дутмаг, мөн ийм бүртгэлийн өгөгдлийг төхөөрөмжийн хадгалалтын хамгаалалттай хэсэгт хадгалахгүй байх нь татгалзахгүй байх баталгааг урьдчилан сэргийлж, хэрэглэгчийг халдлагад өртсөн гэдгээ нотлох боломжгүй болгож чадна. .

e. Аппликешн доторх шифрлэлт дутмаг, буруугаар ашиглагдахаас гадна програмын бүртгэлд аюулгүй байдлаар бичигдсэн эсвэл мэдээллийн санд шифрлэлтгүй эсвэл сул хадгалагдсан байх нь өрсөлдөгчид энэ мэдээллийг ил гаргахад хүргэж болзошгүй юм.

f. Хэрэв програм нь сул шифрийн багцуудыг тохиролцохыг зөвшөөрвөл програм нь сул шифр агуулсан хуучин хувилбарууд руу халдлагад өртөж болзошгүй. Хэрэв сессийн түлхүүрүүдийг үе үе дахин хэлэлцэхгүй бол шифрлэгдсэн материалын хуримтлал нь түлхүүрийг халдлагад өртөмтгий болгодог.

g. Алдагдсан эсвэл хулгайлагдсан хөдөлгөөнт төхөөрөмжид зөвшөөрөлгүй нэвтрэх.

h. Мобайл програмыг өөрчлөх.

3. Хэрэглэгч - DFS агент

a. Үйлчлүүлэгчид SIM солих халдлагад өртөмтгий байж болох бөгөөд халдагчид DFS данс руу нэвтрэх боломжийг олгодог шинэ SIM карт авахын тулд өөрийгөө үйлчлүүлэгчийн хувьд төлөөлөгчийн өмнө төлөөлдөг.

b. Үйлчлүүлэгчийн эрх баталгаажуулалтыг агент хангалтгүй гүйцэтгэсэн эсвэл агент нь халдагчтай нийлж байгаа тохиолдолд DFS данстай холбоотой дагалдах картуудын эсрэг ижил төстэй эмзэг байдал илэрч болно.

4. Хөдөлгөөнт төхөөрөмж - Суурь станц

a. DFS програмууд нь үндсэндээ SMS эсвэл USSD эсвэл IVR ашигладаг GSM сүлжээнүүд нь сүлжээний аюулгүй байдалд тулгуурладаг бөгөөд A5/1, A5/2 зэрэг GSM сүлжээний шифрлэлтийн алгоритмууд дээр суурилдаг. Эдгээр алгоритмууд нь эмзэг болох нь батлагдсан. Сүүлийн үеийн ажил A5/3 шифрийг эвдэхийн тулд ижил төстэй аргуудыг ашиглаж болохыг харуулсан. Зарим системд A5/0 алгоритмыг зааж өгсөн байдаг бөгөөд энэ нь өгөгдлийн нууцлалыг хамгаалахгүй, тэг шифрлэх боломжийг олгодог бөгөөд энэ нь халдагчид агаарын интерфейсээр эмзэг мэдээллийг задлах боломжийг олгодог. Тээврийн сүлжээний аюулгүй байдлын үндсэн аюулаас үл хамааран STK болон https нь төгсгөл хүртэл шифрлэлтийг хангадаг.

b. GSM шифрлэлт (STK, USSD болон IVR) дээр тулгуурласан хуучин сүлжээнүүд нь хууль ёсны үйлчилгээ үзүүлэгчийн цамхаг (жишээ нь, хуурамч суурь станц) гэж хорон санаатайгаар халдагчийн байрлуулсан хуурамч суурь станцуудын "дунд"

халдлагад өртдөг. , ихэвчлэн "IMSI-атагч" гэж нэрлэдэг) ба харилцаа холбоог гар утасны операторын сүлжээнд дахин илгээхийн өмнө шифрийг тайлах. Ийм схем нь халдагчид гүйлгээ, санхүүгийн мэдээлэл зэрэг бүх дамжуулсан мэдээлэлд бүрэн нэвтрэх боломжийг олгоно.

5. Хөдөлгөөнт төхөөрөмж - Интернет

a. Харилцааны холбоосын аюулгүй байдал нь Интернэт дэх төгсгөлийн систем дэх програм болон арын үйлчилгээний хооронд тохиролцсон шифрийн багцаас хамаарна. Аппликешн дэх мэдээлэл нь зөвшөөрөгдсөн төгсгөлийн цэгээс гадуур төрөл бүрийн угаалтуур руу, тэр дундаа бүртгэл, мэдээллийн сан руу урсдаг болохыг харуулсан. Тиймээс зөвхөн TLS гэх мэт хүчтэй шифрлэлтийн механизм нь нийтийн харилцаа холбооны сүлжээнд мэдээллийн аюулгүй байдлыг хангадаг.

b. Ашигласан шифрийн иж бүрдэлүүд нь сул шифр агуулсан хүүчин хувилбаруудад халдлагад өртөхгүй байх нь бас чухал юм. Хэрэв сессийн түлхүүрүүдийг үе үе дахин хэлэлцэхгүй бол шифрлэгдсэн материалын хуримтлал нь түлхүүрийг халдлагад өртөмтгий болгодог. SSL болон тээврийн давхаргын аюулгүй байдал (TLS) зэрэг протоколуудыг шифрийг дахин тохиролцохоор тохируулж болох боловч протоколууд нь үйлчлүүлэгч-серверийн хууль ёсны солилцоо руу траффик оруулж бүй халдагчдын дахин тохиролцооны халдлагад тэсвэртэй байх нь чухал юм. Аюулгүй байдлын түвшинг бууруулсан сул шифрийн багцуудын талаар тохиролцох нь халдагчидад гүйлгээг өөрчлөх, улмаар санхүүгийн мэдээллийн бүрэн бүтэн байдлыг өөрчлөх боломжийг олгоно.

c. Интернэт холболтоор дамжиж буй мэдээллийг зохих шифрлэлтгүйгээр гар утасны төхөөрөмж болон хандалтын цэгийн хоорондох Wi-Fi холбоосоор дамжуулан мэдээллийг чагнаж болно. TLS-ийн гол хэлэлцээрүүдийн эсрэг сүүлийн үеийн халдлагууд нь WPA2 гэх мэт хүчирхэг Wi-Fi протоколууд хүртэл эвдрэлд орох эрсдэлтэй болохыг харуулж байна.

6. Суурь станц-Хөдөлгөөнт шилжих станц - Гарц

a. Дотоод хяналт хангалтгүй байгаа нь хэрэглэгчийн мэдээлэлд нэвтрэх боломжийг олгодог. Энэ нь үйлчилгээ үзүүлэгчийн сүлжээнд шифрлэлт өгдөггүй SMS болон USSD шийдлүүдэд онцгой ач холбогдолтой юм.

b. SS7 сүлжээнд нэвтэрсэн хорлонтой этгээд нь хуурамч сүлжээний түгжрэл, мессежийн чиглэлийг өөрчлөх эсвэл үйлчилгээ/холбоосыг ашиглах боломжгүй болгохын тулд Message Transfer Part (MTP) удирдлагын мессежийг илгээж болно.

c. Үүрэн холбооны сүлжээ нь SS7 холбоосыг хэт ачаалснаар гүйцэтгэх боломжтой Үйлчилгээнээс татгалзах (DoS) аюулд өртөмтгий байдаг. Халдагчид маш их боловсруулалт шаарддаг SCCP (Дохионы холболтын хяналтын хэсэг) хүсэлтийг илгээдэг, жишээ нь Global Titles-ийн орчуулга.

d. Мэдээллийг дотоод хүмүүс, ялангуяа мессежийн бүрэн бүтэн байдлын тухай ойлголтгүй протоколд хууран мэхлэх боломжтой.

e. SS7 сүлжээнд нэвтрэх хялбар байдал нь халдагчид MAP (Mobile Application Part) үйлдлүүдийг ашиглан захиалагчийн өгөгдлийг оруулах, өөрчлөх, гар утасны холбоо барих, захиалагчийн байршлыг тодорхойлох боломжийг олгодог.

f. Хөдөлгөөнт бааз станц болон үйлчилгээ үзүүлэгчийн сүлжээний хоорондох холбооны холбоос нь зарим тохиолдолд утастай холбоо байдаг бол зарим тохиолдолд гар утасны сүлжээний топографаас хамааран үндсэн станцууд нь богино долгионы гэх мэт үйлчилгээ үзүүлэгчийн сүлжээнд утасгүй холбогдож болно. холбоос. Хэрэв энэ харилцаа холбоо шифрлэгдээгүй бол, ялангуяа гар утас болон үндсэн станцын хооронд GSM алгоритмаар шифрлэлтийг хатуу хангадаг SMS болон USSD-д суурилсан гүйлгээний хувьд тухайн өгөгдлийг сүлжээнд тодорхой байдлаар буцааж илгээж, нууцлалыг зөрчихийг хөнгөвчлөх боломжтой.

g. DFS контекстэд SS7 сүлжээний түвшний хандалттай баталгаагүй хэрэглэгч эсвэл хуурамч дугаар (CLI)-аар DFS харилцагч руу залгаж, DFS болон банкны баталгааг DFS-ээс авахыг оролдох боломжтой. Эцэст үйлчлүүлэгчийг санхүүгийн алдагдалд хүргэдэг.

h. MNO-ийн хэрэглэгчид зөвшөөрөлгүй SIM солилцооны золиос болох ба халдагчид SS7-ийн халдлагаас олж авсан захиалагчийн мэдээллийг ашиглан SIM сольж мэдээллийг олж авах эсвэл MNO-ийн дотоод ажилтнуудтай хамтран ажиллах боломжтой.

i. MNO доторх давуу эрхтэй хэрэглэгчид HLR болон MSC зэрэг үндсэн зангилаа руу нэвтрэх эрхээ урвуулан ашиглаж дуудлага, SMS дамжуулах, дуудлага дамжуулах, зөвшөөрөлгүй таслах, DFS захиалагчийн дуудлагын өгөгдлийн бүртгэлийг цуглуулах зэрэг үйлдлүүдийг хийх боломжтой.

7. Үүрэн холбооны сүлжээ - DFS оператор

a. Мэдээллийг үйлчилгээ үзүүлэгчийн сүлжээнд дамжуулсны дараа өгөгдлийг хамгаалах, ялангуяа өгөгдлийг шифрлэх арга зам нь ихэвчлэн бага байдаг. Сүлжээнд шифрлэгдсэн өндөр зурвасын холболтыг хадгалахад шаардагдах тооцооллын зардал болон нэмэлт зардал зэрэг олон шалтгаан бий. Сүлжээнд үчирч буй аюул занал нь дотроос бус гаднаас үүсдэг

гэсэн таамаглал ч байдаг. Үүний үр дүнд сүлжээнд нэвтэрч чадах дотоод өрсөлдөгчид болон гадны аюул заналхийллийн аль алинд нь эмзэг байдал бий болно.

b. Эдгээр сүлжээн дэх бүрэн бүтэн байдлын хамгаалалт байхгүйгээс операторын сүлжээн дэх өгөгдөл эрсдэлд ордог. Сүлжээнд нэвтрэх чадвартай өрсөлдөгч (жишээ нь, периметрийн хамгаалалтыг зөрчих замаар) эсвэл хорлонтой инсайдер ийм мэдээллийг дур зоргоороо өөрчилж болно.

c. Аюулгүй байдлын элемент болгон SIM болон SIM/гар утасны дугаарыг санхүүгийн данс болгон ашигладаг DFS үйлчилгээ үзүүлэгчид SIM картыг дахин боловсруулах явцад дансаа алдах магадлалтай. Хэрэв GSM сүлжээнд тодорхой хугацаанд идэвхгүй/идэвхгүй байсан бол гар утасны дугаараа шинэ хэрэглэгчдэд шилжүүлж, үе үе SIM дахин боловсруулалт хийдэг үүрэн холбооны операторууд, SIM картыг дахин боловсруулах үйл явц нь санхүүгийн данс руу нэвтрэх эрхээ алдаж болзошгүй. түүнийг өөр хэрэглэгч рүү хууль бусаар шилжүүлэх.

d. MNO төхөөрөмжийн тохиргоо болон хүчин чадлын хязгаарлалт нь дижитал санхүүгийн үйлчилгээний үйлчилгээ, хүртээмжийг хязгаарлаж, USSD сессийн уртын хязгаарлалт нь DFS гүйлгээг тасалдуулж болзошгүй юм.

e. Үүрэн холбооны операторын сүлжээ болон физик дэд бүтцийн өргөн цар хүрээ нь түүнийг зөвшөөрөлгүй алсын зайнаас нэвтрэх боломжийг олгодог хуурамч төхөөрөмжүүдийг суулгаснаар эвдрэлд өртөмтгий болгодог бөгөөд DFS экосистемийн харилцан уялдаатай байдал нь хуурамч хандалттай хүмүүст MNO-ээс гадна өөр өөр оролцогч талуудад хандах боломжийг олгодог.

f. Агаарын интерфэйс ба MSC-ийн хөндлөнгийн оролцоо: MSC нь хууль ёсны хөндлөнгийн оролцоог зөвшөөрөх чадвартай, MSC-д давуу эрхээр хандах нь харилцаа холбоог таслан зогсоох боломжтой гэсэн үг бөгөөд энэ хандалтыг DFS-ийн үйл ажиллагааг хянах эсвэл үгүйсгэх замаар санхүүгийн хуурамч ашиг олох зорилгоор ашиглаж болно.

g. Үүрэн холбооны сүлжээн дэх үйлчилгээний халдлагыг үгүйсгэх, MSC гарц гэх мэт операторуудын зангилаа IP ашиглан бусад сүлжээний операторуудтай холбогдож байгаа нь энэ эрсдэлийг нэмэгдүүлдэг бөгөөд энэ нь үеийн болон нөөцийн халдлагад өртөх эрсдлийг нэмэгдүүлдэг бөгөөд энэ нь ихэвчлэн ирж буй траффикийн хэмжээг нэмэгдүүлж, хэт ачааллахад хүргэдэг. IP стек болон зангилааны процессорууд нь зангилааг зогсоох эсвэл дахин эхлүүлэхэд хүргэдэг бөгөөд энэ нь бэлэн байдалд шууд нөлөөлдөг.

h. Дуудлагын чиглэлийг өөрчлөх, дамжуулах; Гадны халдагчид хандах эрх олж авах эсвэл Сүлжээний төхөөрөмжид хандах эрхтэй нэг нь DFS холболтыг өөр дугаар руу шилжүүлж болох бөгөөд үүнийг гар утасны захиалагчийн гэрийн байршлын профайлыг өөрчлөх замаар халдагчид DFS-ийн нууц мэдээлэлд хандах боломжийг олгож болно.

8. DFS оператор - Гуравдагч этгээд

a. Шифрлэлт нь үйлчилгээ үзүүлэгчийн сүлжээн дотор болон хооронд хатуу ажиллахгүй бол өгөгдөлд өртөх болно. Аюул нь үйлчилгээ үзүүлэгчийн сүлжээний периметрийн гаднаас (өөрөөр хэлбэл гадаад сүлжээ) олж авсан мэдээллээс үүсдэг бол дотоод аюул нь сүлжээний периметр дотор (өөрөөр хэлбэл дотоод сүлжээ) байдаг. Нэмж дурдахад, үйлчилгээ үзүүлэгчийн сүлжээн дэх системүүд сүлжээгээр болон хост системд холбосон хортой захын төхөөрөмжөөр (жишээ нь, гарт суулгасан хортой USB флаш диск эсвэл keylogger) дамжуулж болох хортой програмаар халдварласан тохиолдолд өгөгдөл ил болно. Ийм төхөөрөмжүүд нь үйлчилгээ үзүүлэгчийн орчноос өгөгдлийг халдагч руу буцаан шилжүүлж чаддаг.

b. Гадны үйлчилгээ үзүүлэгчийн мэдээллийн санд нэвтрэх боломжтой халдагчид, тухайлбал, програм хангамжийн эмзэг байдлыг алдагдуулах замаар санхүүгийн мэдээлэл болон үйлчилгээ үзүүлэгчийн нууц мэдээллийг өөрчлөх чадвартай байдаг. Ялангуяа сүлжээнүүдийн хоорондын интерфейс нь халдагчид нэвтрэх боломжит цэг болж өгдөг бөгөөд үүнийг сайтар хянаж байх ёстой. Нэмж дурдахад, амарч буй өгөгдөл нь эдгээр мэдээллийг хадгалдаг хостууд болон серверүүд дээр тавьсан хамгаалалттай адил аюулгүй байдаг.

c. Аюулгүй байдлын шинэчлэлтүүд нь нарийн шинэчлэгдээгүй DFS сервер нь хортой програм болон rootkit-ийн хохирогч болж болзошгүй. Нийтийн сүлжээний интерфейстэй тулгарсан бүх машинууд өмнө нь хэзээ ч байгаагүй "тэг өдрийн" халдлага зэрэг сүлжээнд суурилсан мөлжлөгт өртөж болзошгүй. Мөн CD/DVD хөтчүүд, USB портууд болон бусад захын интерфейсүүд гэх мэт бусад оролт гаралтын интерфэйсүүдээр дамжуулан системүүд нь хортой код болон өгөгдөл оруулах боломжтой байдаг.

d. Анхдагч хандалт болон нууц үгийн тохиргоо, идэвхтэй чухал бус үйлчилгээ, telnet болон ftp зэрэг идэвхтэй хамгаалалтгүй протокол, файлд хандах зөвшөөрөл, сүлжээний анхдагч тохиргоо, хэн унтраахыг зөвшөөрөх зэрэг хэрэглэгчийн эрх зэрэг DFS үйлдлийн системийг хатуурууллахад хангалтгүй байдал.

e. CD, DVD, USB гэх мэт гадаад ачаалах төхөөрөмжүүдэд хяналтгүй нэвтрэх, BIOS-д нууц үгүйгээр нээлттэй нэвтрэх нь DFS системд халддаг талбар юм.

Тайлбар:

1 https:// globalfindex .worldbank .org/

2 ITU-T Focus Group Digital Financial Services, Digital Financial Services Security Aspects, 2017 оны 1-р сар, https:// www .itu .int/ en/ ITU -T/ studygroups/ 2017 -2020/ 09/ Баримт бичиг/ ITU _FGDFS _SecurityReport .pdf

3 https:// www .ecb .europa .eu/ paym/ pdf/ cons/ cyberresilience/ Cyber _resilience _oversight _expectations for _financial _зах зээлийн дэд бүтэц .pdf

4 Том өгөгдлийн ML ба хэрэглэгчийн нууцлалын талаарх тайлан нь эрсдэл болон хэрэглэгчийн санхүүгийн болон харилцаа холбооны мэдээллийг хэрхэн бууруугаар ашиглаж болохыг онцолдог.

5 DFS-ийн SS7-ийн эмзэг байдал, нөлөөллийг бууруулах арга хэмжээний тухай Техникийн тайланг үзнэ үү – Хэсэг 12.5 SIM картыг дахин ашиглахыг илрүүлэх, урьдчилан сэргийлэх, багасгах

6 SS7-ийн эмзэг байдал болон DFS-ийн нөлөөллийг бууруулах арга хэмжээний тухай Техникийн тайланг үзнэ үү – Тайлангийн 8, 9-р хэсгийг үзнэ үү.

7 DFS-д зориулсан SS7-ийн эмзэг байдал болон нөлөөллийг бууруулах арга хэмжээний тухай Техникийн тайланг үзнэ үү – Хэсэг 12.1 Таслагдсан OTP SMS ашиглан данс бүлаалтыг илрүүлэх, багасгах

8 DFS-д зориулсан SS7-ийн эмзэг байдал болон нөлөөллийг бууруулах арга хэмжээний тухай Техникийн тайланг үзнэ үү – Үүрэн холбооны операторуудад үзүүлэх нөлөөллийг бууруулах стратеги 10-р хэсгийг үзнэ үү.

9 GSM холбоо, албан ёсны баримт бичиг MM.01 – MM Апп аюулгүй байдлын шилдэг туршлагууд, 1.0 хувилбар, 2018 оны 6-р сарын 28.

10 Европын холбооны кибер аюулгүй байдлын агентлаг (ENISA), Ухаалаг гар утасны аюулгүй байдлын хөгжлийн удирдамж, 2017 оны 2-р сарын 10.

11 Пакистаны Төрийн банк, Мобайл төлбөрийн хэрэглүүрийн (апп) аюулгүй байдлын хүрээ (DRAFT хувилбар 1.0), 2019 оны 4-р сар.

12 https:// www .cisecurity .org/ controls/ insident -response -and -management/

International Telecommunication Union
Place des Nations
CH-1211 Geneva 20
Switzerland