ХАРИЛЦАА ХОЛБООНЫ ЗОХИЦУУЛАХ ХОРОО

30 ЖИЛ

# NATIONAL ANTI-FRAUD SYSTEM (NAS)

ЗГ, ТХТ-ийн мэргэжилтэн Ц.Нямсүрэн

# АГУУЛГА

## 01 ЗАЛИЛАНГИЙН ӨНӨӨГИЙН НӨХЦӨЛ БАЙДАЛ

- Өнөөгийн нөхцөл байдал
- Залилангийн эсрэг бодлого, чиг хандлага

## 02 ЗАЛИЛАНГИЙН ЭСРЭГ ҮНДЭСНИЙ НЭГДСЭН СИСТЕМ (NAS)

- National anti-fraud system
- Монгол Улсад хэрэгжүүлэх NAS-ийн туршилтын загвар (POC)
- Монгол Улсад хэрэгжүүлэх IM Deactivation шийдлийн туршилтын загвар (POC )

# ӨНӨӨГИЙН НӨХЦӨЛ БАЙДАЛ

## ЗАЛИЛАН -ДЭЛХИЙН ХЭМЖЭЭНИЙ АЮУЛ

**Кибер гэмт хэргийн** (цахим орчинд эсвэл сүлжээнд холбогдсон төхөөрөмжөөр хийгдэх гэмт хэрэг) үүнд залилан орно, дэлхийн хэмжээнд учруулах санхүүгийн хохирлын хэмжээ 2024 онд **9.22 их наяд ам.доллар** байгаа бол 2029 он гэхэд **15.63 их наяд ам.доллар** хүртэл өсөхөөр төлөвлөгдөж байна. *(Statista[1])*

2023 оны эцсийн байдлаар дэлхий даяар **5.6 тэрбум хүн** (хүн амын 69%) гар утасны үйлчилгээ ашиглаж, **4.7 тэрбум хүн** (хүн амын 58%) мобайл интернет хэрэглэж байна (*GSMA Mobile Economy Report*, 2024[2]).

2023 онд гэмт хэрэгтнүүд хорирогчдод **1 их наяд ам.долларааc** давсан хохирол учруулжээ. *(Global Anti-Scam Alliance[3])*

Дэлхийн байгууллагуудын **71%** нь 2023 онд и-мэйл дээр суурилсан **Phishing** халдлагад дор хаяж нэг удаа өртсөн байна. (*Proofpoint's 2023 State of the Phish Report[4]*)

# ӨНӨӨГИЙН НӨХЦӨЛ БАЙДАЛ

## ЗАЛИЛАНГИЙН НИЙТЛЭГ ТӨРЛҮҮД

**Authorised Push Payment fraud (Зөвшөөрөгдсөн шилжүүлгийн залилан)**
Итгэмжлэгдсэн байгууллага (жишээ нь банк) мэтээр хуурч, хохирогчоор өөрийн данс руугаа мөнгө шилжүүлүүлэх залилан.

**Baiting- (Өгөөш)**
Гэмт этгээд уруу татах зүйл санал болгож хохирогчийг хортой файлыг татуулах эсвэл системд нэвтрэх боломж олгох. Үүнд халдварласан дижитал файл эсвэл линк орно.

**Business Email Compromise (Бизнес имэйлийн залилан)**
Бизнесийн имэйл дансанд нэвтэрч, гүйлгээг өөрчилж эсвэл нууц мэдээллийг хулгайлан мөнгө завших хэлбэрийн халдлага.

**Identity fraud (Хувийн мэдээлэл ашиглан хийх залилан)**
Өөр хүн болж жүжиглэх, эсвэл хуурамч нэр, хувийн мэдээлэл ашиглан хуурч мэхлэх.

**Identity theft (Хувийн мэдээлэл хулгайлах)**
Хувийн мэдээллийг хулгайлж, түүнийг ашиглан данс нээх, худалдан авалт хийх гэх мэт гэмт үйлдэл хийх.

**Impersonation (Өөр хүний дүрээр үйлдэх залилан)**
Утас, имэйл, мессежээр өөр хүн эсвэл байгууллага болж хуурч, мөнгө, мэдээлэл авах зорилготой үйлдэл.

**Phishing (Мэхлэх залилан)**
Хуурамч имэйл, мессеж, сошиал медиа дамжуулан хэрэглэгчээс нууц үг, дансны дугаар зэрэг мэдээллийг авах зорилгоор итгэмжлэгдсэн байгууллага мэтээр хуурч мэхлэх.

**Pretexting (мэхэлж мэдээлэл авах)**
Хуурамч нөхцөл байдал үүсгэж, мэдээлэл авах зорилгоор итгэмжлэгдсэн хүн болж жүжиглэх (жишээ нь хамт ажиллагсад, банкны төлөөлөгч).

**Robocall (Автомат дуудлага)**
Урьдчилан бичсэн мессежтэй автомат дуудлага ашиглан залилан хийх. Жишээлбэл, хуурамч санал, төлбөрийн мэдээлэл авах оролдлого.

**SIM Swap fraud (SIM солиулах залилан)**
Гар утасны үйлчилгээ үзүүлэгчийг хуурч, хохирогчийн дугаарыг шинэ SIM карт руу шилжүүлж, түүний дуудлага, мессеж, баталгаажуулалтын кодыг авах.

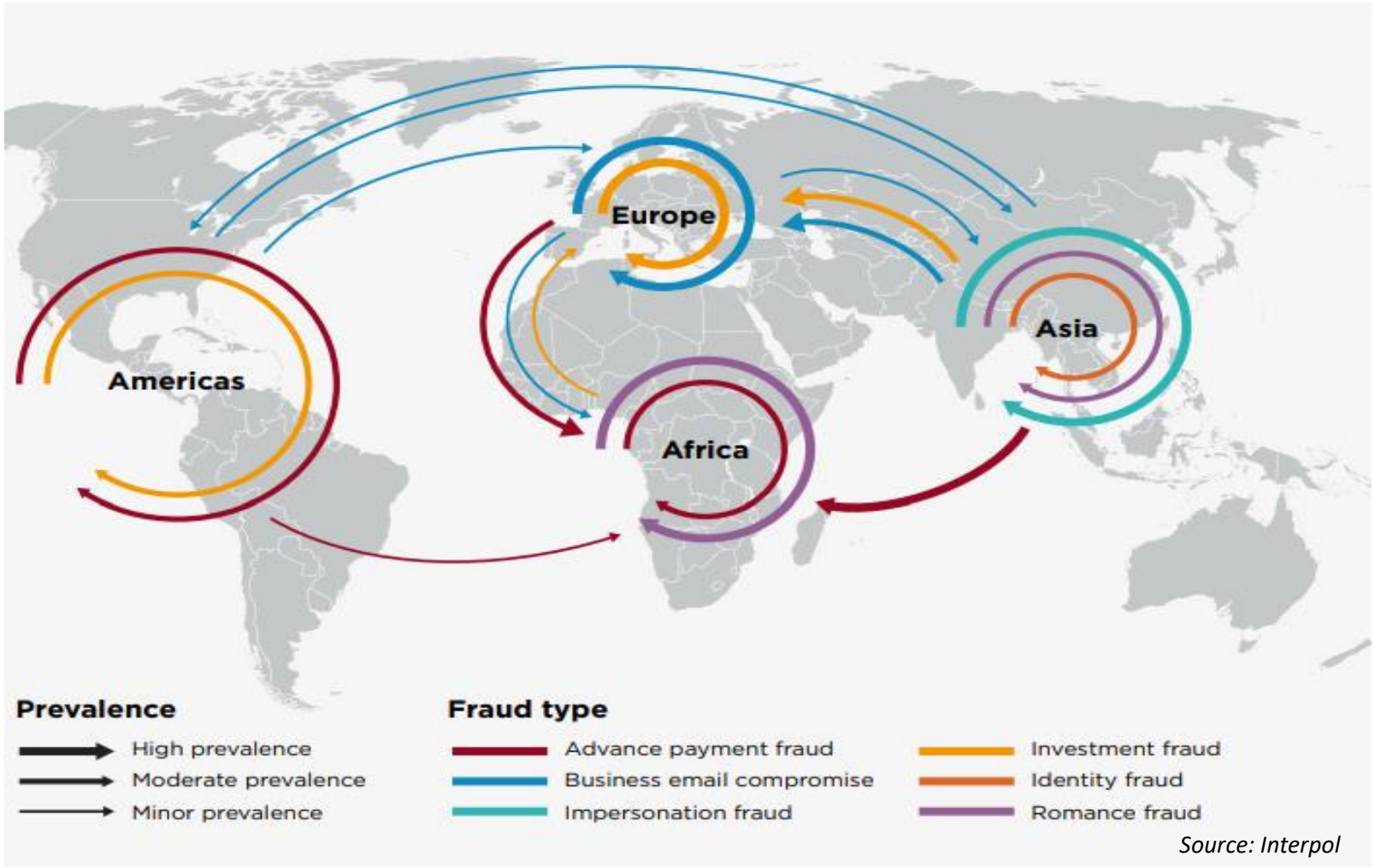
**Smishing and Vishing (Смишинг ба Вишинг)**
- **Smishing**: SMS ашиглан хувийн мэдээлэл авах оролдлого.
- **Vishing**: Утасны дуудлагаар мэдээлэл авах оролдлого.

**Spear phishing (Тодорхой чиглэлийн фишинг)**
Тодорхой хүн эсвэл байгууллагыг урьдчилан судалж, мэдээлэлд чиглэсэн фишинг халдлага.

**Spoofing (хуурамч дугаар, IP хаяг харуулах)**
IP хаяг, дугаар, имэйл хаяг зэрэг мэдээллийг хуурамчаар өөрчилж, өөр эх сурвалж мэт харагдуулан хуурч мэхлэх.

# ӨНӨӨГИЙН НӨХЦӨЛ БАЙДАЛ

## ДЭЛХИЙН БҮС НУТГУУД ДАХЬ САНХҮҮГИЙН ЗАЛИЛАНГИЙН ЧИГ ХАНДЛАГА




*Source: Interpol*

**Интерполын санхүүгийн залилангийн судалгаанд:**

• **Африк, Ази, Латин Америкт:** SIM swap, SIM солих, хувийн мэдээллийг залилах түгээмэл байгаа бол **Европт:** хөрөнгө оруулалтын луйвар, бизнесийн имэйл залилан, романтик залилан, мөн phishing залилан хамгийн түгээмэл халдлагын арга хэвээр байна.

Сошиал инженерчлэлийн залилантай тэмцэхийн тулд **засгийн газрууд, зохицуулагч байгууллагууд** болон мобайл салбар нь хууль эрх зүйн, зохицуулалтын, техникийн болон боловсролын олон **арга хэмжээг хэрэгжүүлж** байна.

# ЗАЛИЛАНГИЙН ЭСРЭГ БОДЛОГО, ЧИГ ХАНДЛАГА

## ЗАЛИЛАНГИЙН ЭСРЭГ ОЛОН ТАЛТ АРГА ХЭМЖЭЭ

**Боловсрол, мэдлэг олгох кампанит ажил**

- Олон нийтийн мэдлэгийг нэмэгдүүлэх, мэдээлэлээр хангах кампанит ажил зохион байгуулж байна.
- Мобайл операторууд ажилчиддаа сургалт явуулж, хэрэглэгчдэд зориулсан хамгаалалтын зөвлөгөөг вебсайтаараа дамжуулан түгээж байна. Жишээ: **UK & Canada:** хэрэглэгчид 7726 дугаараар spam/fraud SMS, дуудлага мэдээлдэг.

**Техникийн арга хэмжээ**

- Firewall хамгаалалт болон баталгаажуулах механизм
- Мэдээллийн аюулгүй байдлын бодлого, системийн **тогтмол хяналт**, тайлан
- SMS Sender ID хамгаалалтын бүртгэл — байгууллагууд өөрсдийн илгээдэг мессежийн гарчгийг бүртгүүлж хамгаалснаар SMS phishing болон spoofing-ийн эрсдлийг бууруулдаг.
- **Салбар хоорондын хамтын ажиллагаа** болон **API** суурьтай шийдлүүд нь банкны болон дижитал залилангийн эсрэг тэмцэх гол арга зам болж байна. Жишээлбэл: **Их Британид** GSMA болон UK Finance хамтран банкууд болон мобайл операторуудын **Scam Signal** шийдэл**, Ази Номхон далай, Латин Америк** зэрэг бүс нутагт операторууд **Open Gateway API** ашиглан банкны залиланг зогсоох боломжийг бүрдүүлжээ.

**Мобайл мөнгөн гүйлгээний залилангийн эсрэг тэмцэл**

GSMA-ийн **“Mobile Money fraud typologies and mitigation strategies”** тайланд мобайл мөнгөний луйврын төрөл, чиг хандлага, луйварчдын арга барил болон урьдчилан сэргийлэх, илрүүлэх, хариу **арга хэмжээ авах стратегийг** тусгасан.

- **Number Verify** –хэрэглэгч зөвхөн бүртгэгдсэн **дугаартай төхөөрөмжөөс хандаж** буй эсэхийг баталгаажуулдаг тул нэмэлт код, нууц үгийн шаардлагагүйгээр найдвартай нэвтрэх боломжийг олгодог.
- **SIM Swap** – SIM карт сүүлд хэзээ **солигдсоныг шалгаж**, сэжигтэй өөрчлөлт илрүүлэн таних нь залилангаас сэргийлнэ.
- **Device Location Verification** –Төхөөрөмж тухайн байршилд байгаа эсэхийг баталгаажуулна.
- **Know Your Customer (KYC)** – хэрэглэгчийн мэдээллийг mobile network-ээр хурдан шалгаж, бүртгэлийг аюулгүй болгодог.

# ЗАЛИЛАНГИЙН ЭСРЭГ БОДЛОГО, ЧИГ ХАНДЛАГА

## ЗАЛИЛАНГИЙН ЭСРЭГ ОЛОН ТАЛТ АРГА ХЭМЖЭЭ

**GSMA Open Gateway-ийн хүрээнд** мобайл операторууд Mobile Connect болон **API-уудыг ашиглан** хэрэглэгчийн баталгаажуулалт, дижитал аюулгүй байдлыг сайжруулж, **онлайн залилангийн эсрэг хамтын ажиллагаа** өрнүүлж байна. Энэ хүрээнд **Малайз, Сингапур, Тайланд** зэрэг орнуудад хамтын ажиллагаа идэвхтэй өрнөж байна.

Дэлхий даяар **операторууд** Number Verification, SIM Swap, KYC Match **стратеги** болон **API**-уудыг нэвтрүүлж, **залилангийн эрсдэлийг бууруулах** чиглэлд ажиллаж байна. **GSMA** нь мөн One Consortium санаачилга болон Mobile Cybersecurity Knowledge Base, FASG, T-ISAC зэрэг платформоор дамжуулан spam, spoofing-ийг бууруулах, мөн fraud/scam-ийн талаарх мэдээлэл**, туршлага, зөвлөмжийг гишүүн операторуудын** хооронд **хуваалцах боломжийг** хангаж байна.

### Хууль эрх зүйн болон зохицуулалтын арга хэмжээ

Дэлхий даяар залилангийн үйл ажиллагааг төрөл бүрийн хууль, зохицуулалтаар шийдвэрлэж байгаа бөгөөд тухайн улсын хууль эрх зүйн орчин харилцан адилгүй байдаг. Зарим улс оронд тусгай хууль батлагдсан байдаг.

- **Их Британи** – *Fraud Act 2006* нь залиланг шууд чиглэсэн гэмт хэрэгт тооцдог;
- **Австрали**-д *Scams Prevention Framework* хэрэгжүүлэх хууль шинээр батлагдаж байгаа бөгөөд энэ нь засгийн газарт банк, харилцаа холбоо, нийгмийн сүлжээ болон мессежийн **үйлчилгээ үзүүлэгч** зэрэг салбаруудыг **“залилангийн өндөр эрсдэлтэй”** гэж ангилж, **тусгай хамгаалалтын зохицуулалт** хэрэгжүүлэх боломж олгож байна.
- Олон улс оронд **KYC шаардлага, гүйлгээний хяналт, хэрэглэгчийн зан төлөвийн шинжилгээ** зэрэг antifraud **системийг** заавал **нэвтрүүл**ж, байгууллагууд хоорондоо **мэдээлэл солилцон хил дамнасан залилангаас сэргийлэхэд** хамтран ажиллаж байна.
- **Австрали** улсад нэвтрүүлж буй **“Scam Code”** нь телеком болон санхүүгийн **байгууллагуудын үүргийг тодорхойлон**, залилан илэрмэгц сэжигтэй дуудлага хаах, данс царцаах зэрэг **шуурхай арга хэмжээ авах** боломжийг бүрдүүлдэг.

# ЗАЛИЛАНГИЙН ЭСРЭГ БОДЛОГО, ЧИГ ХАНДЛАГА

## Дүрэм журам

Олон улсын хууль, тогтолцоонууд уялдаа холбоотой болж, улс орнууд мэдээлэл солилцож, кибер болон залилангийн гэмт хэргийн эсрэг хамтран ажиллах **олон улсын гэрээ, конвенц, хамтын ажиллагааны механизм** бий болгосон

•**Малабо конвенц** нь **Африк тивийн** кибер аюулгүй байдал, мэдээлэл хамгаалалтын нэгдсэн **хууль эрхзүйн тогтолцоог бүрдүүлж**, хувийн мэдээллийн хулгай зэрэг үйлдлийг гэмт хэрэгт тооцдог бөгөөд **15 улс** баталснаар 2023 оны 6-р сард хүчин төгөлдөр болсон.

•АНУ-ын FTC, мөн **Латин Америкийн зарим улс (**Чили, Колумб, Мексик, Перуги)-ийн хэрэглэгчийн эрхийг хамгаалах байгууллагууд залилангийн эсрэг тусгай механизм бий болгосон.

•**GSMA**-гийн дэмжлэгтэйгээр **Европын зохицуулагч** байгууллагуудын хамтын ажиллагааг хөгжүүлэх зорилготой **GIRAF** (Global Informal Regulatory Antifraud Forum) хэрэгжиж байна.

•**Европын Зөвлөлийн Будапештийн конвенц** нь кибер гэмт хэрэгт олон улсын хамтын ажиллагааны **хууль эрхзүйн суурь** болж, онлайн залилан болон хувилбарлан үйлдэх схемийн мөрдөн шалгалтыг дэмждэг.

•2024 оны 8-р сард **НҮБ** гишүүн орнуудад кибер гэмт хэрэг, залилангийн үйлдлийг гэмт хэрэгт тооцох үүрэг оноосон бөгөөд энэ нь нотлох баримт солилцох, хөрөнгө хураах зэрэг **хил дамнасан хамтын ажиллагааг** шаарддаг.

## Салбар хоорондын хамтын ажиллагаа ба мэдээлэл солилцоо

Залилангийн эсрэг тэмцэлд ганц байгууллага эсвэл салбар дангаараа хангалтгүй тул **салбар хоорондын хамтын ажиллагаа, бодит цагийн өгөгдөл, нөөцөө нэгтгэснээр** залиланг хурдан илрүүлж, таслан зогсоох боломжтой болсон.

•**Их Британи** – Засгийн газар ба томоохон технологийн компаниуд онлайн залилангаас хамгаалах амлалт хийсэн.

•**Австрали** – Anti-Scam Centre байгуулсан.

•**Европ, ASEAN** – санхүүгийн байгууллага, мобайл оператор, хууль сахиулах байгууллагуудын хооронд **хил дамнасан шууд харилцааны суваг** нээсэн.

**Энэтхэг** – DoT операторуудтай хамтран олон улсын spoofing дуудлагыг хэрэглэгчдэд хүрэхээс өмнө блоклодог.

**АНУ** – Robocall хамгийн их гомдлын шалтгаан болж, FCC болон FTC-д олон мянган гомдол үүсгэсэн.

# ӨНӨӨГИЙН НӨХЦӨЛ БАЙДАЛ

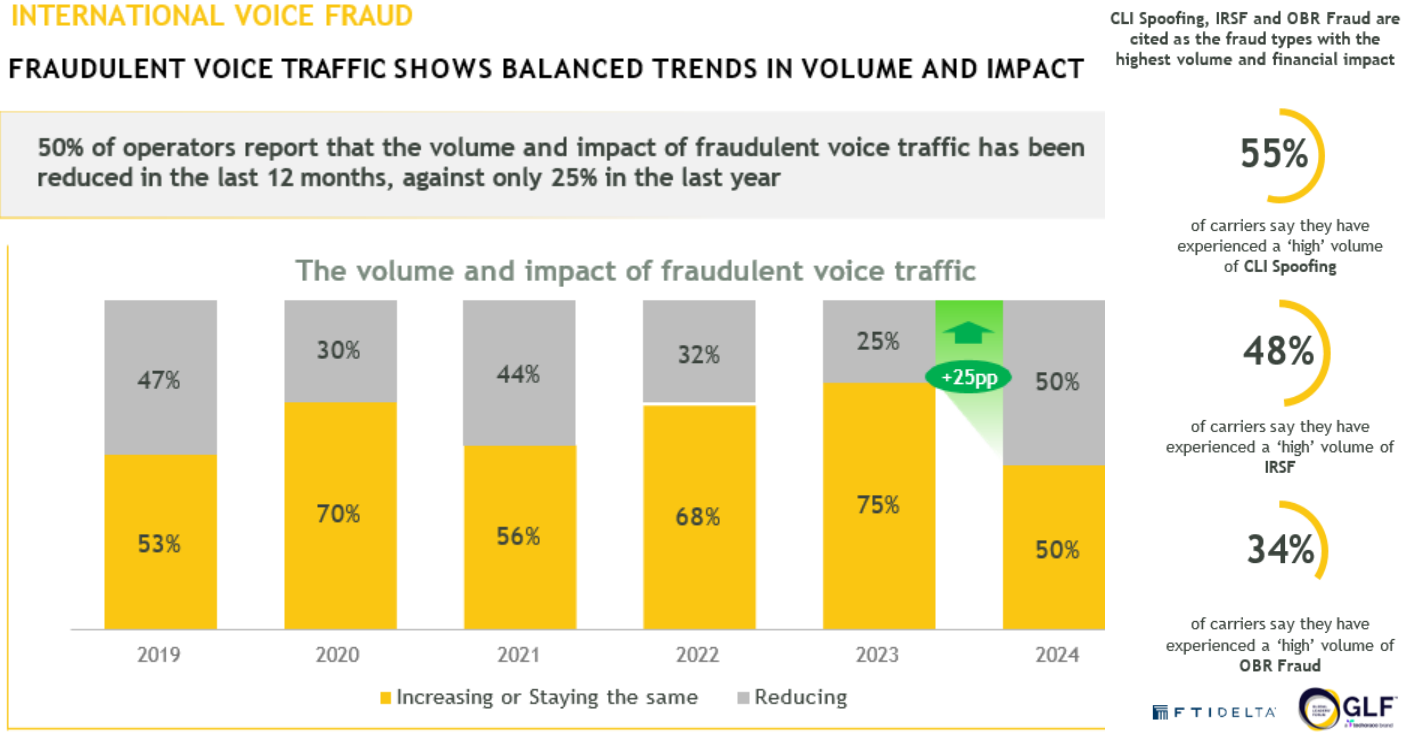

Харилцаа холбооны салбар жил бүр ихээхэн хэмжээний **хохирол дагуулдаг** залилангийн асуудалтай тулгардаг бөгөөд үүний дийлэнхийг **дуудлага болон SMS**-ийн харилцан холболтын залилан эзэлдэг.

***GLF FRAUD REPORT 2024*** тайланд, харилцаа холбооны салбар дахь **залилангийн нөхцөл** байдал болон чиг хандлагыг нэгтгэн дүгнэсэн.

Тайланд оролцсон операторуудын бараг **гуравны хоёр** нь залилангийн эсрэг тэмцлийг “**нэн тэргүүний зорилт**” гэж үзжээ.

Тайланд мөн залилангийн эсрэг тэмцэлд салбар хоорондын үр дүнтэй **хамтын ажиллагаа**, мэдээлэл солилцоо болон **нэгдсэн стратеги** боловсруулах нь зайлшгүй чухлыг онцолсон байна.

# ӨНӨӨГИЙН НӨХЦӨЛ БАЙДАЛ




**Гол төрлийн залилан**

- **CLI Spoofing (Caller Line Identification Spoofing)- 55%**

*Утасны дугаарыг хуурамчаар өөрчлөн итгүүлэх залилан*

- **IRSF (International Revenue Share Fraud) -48%**

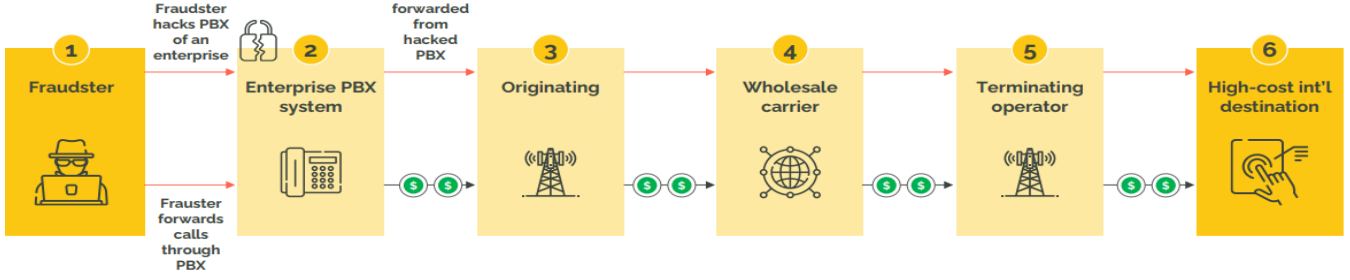
*Залилагчид өндөр тарифтай олон улсын **тусгай дугаар эзэмшигчидтэй хамтран орлого хуваах зорилготой** залилан үйлдэг.*

- **OBR залилан (Out Bound Refile Fraud)-34%**

*Бодит өртгөөс хямд тарифаар төлбөр тооцоо хийхийн тулд дуудлагын чиглэл, **тарифыг санаатайгаар өөрчилдөг.***

- **Wangiri 2.0 (Call-Back залилан)**–*Залилагч нэг удаа залгаад шууд тасалж, байгууллага эсвэл хэрэглэгчийг өндөр тарифтай дугаар руу буцаан залгуулахад хүргэдэг.*

**PBX хакердах**–Залилагчид байгууллагын дотоод утасны (PBX) системд хууль бусаар нэвтэрч, зөвшөөрөлгүйгээр өндөр тарифтай олон улсын дуудлага хийгдэж, байгууллагад их хэмжээний төлбөрийн хохирол учруулж байна.




***Эрсдэлийг бууруулах шийдэл:***

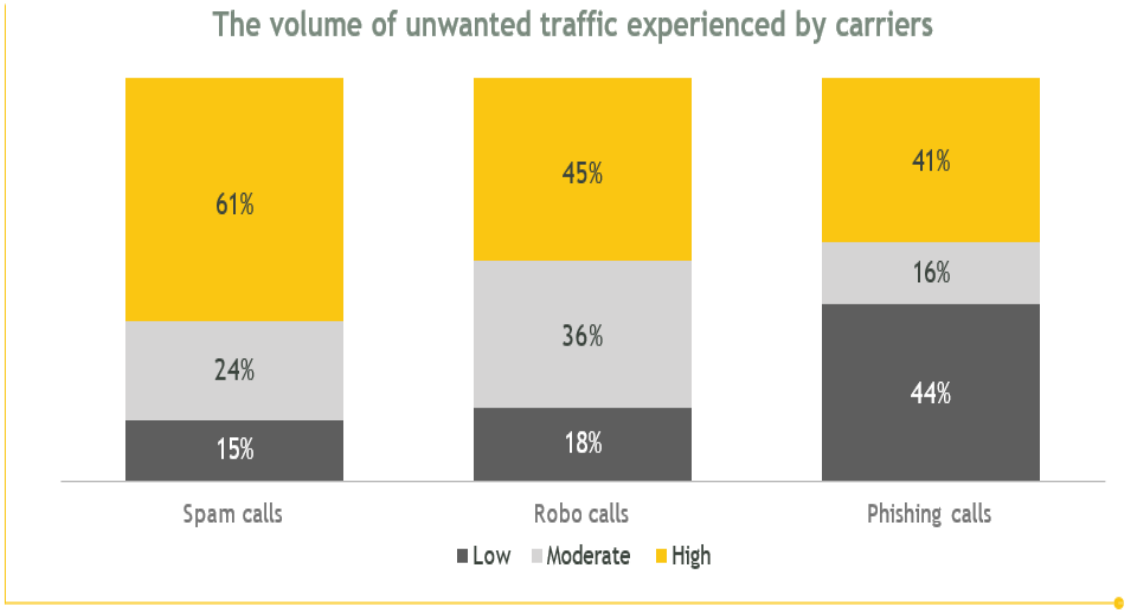
- *Дуудлагын эх сурвалжийг баталгаажуулах*
- *Бодит цагийн хяналт*
- *Автоматаар блоклох*
- *Хэрэглэгчийн сэрэмжлүүлэг*
- ***Системийн хамгаалалт***
- *Аудитын арга хэмжээг хэрэгжүүлэх шаардлагатай.*

# ӨНӨӨГИЙН НӨХЦӨЛ БАЙДАЛ

## UNWANTED TRAFFIC

### SPAM CALLS LEAD UNWANTED TRAFFIC, OUTPACING ROBO AND PHISHING CALLS

More than 40% of carriers report getting high volumes of nuisance calls, i.e., spam calls, robo calls and phishing calls




**76%**

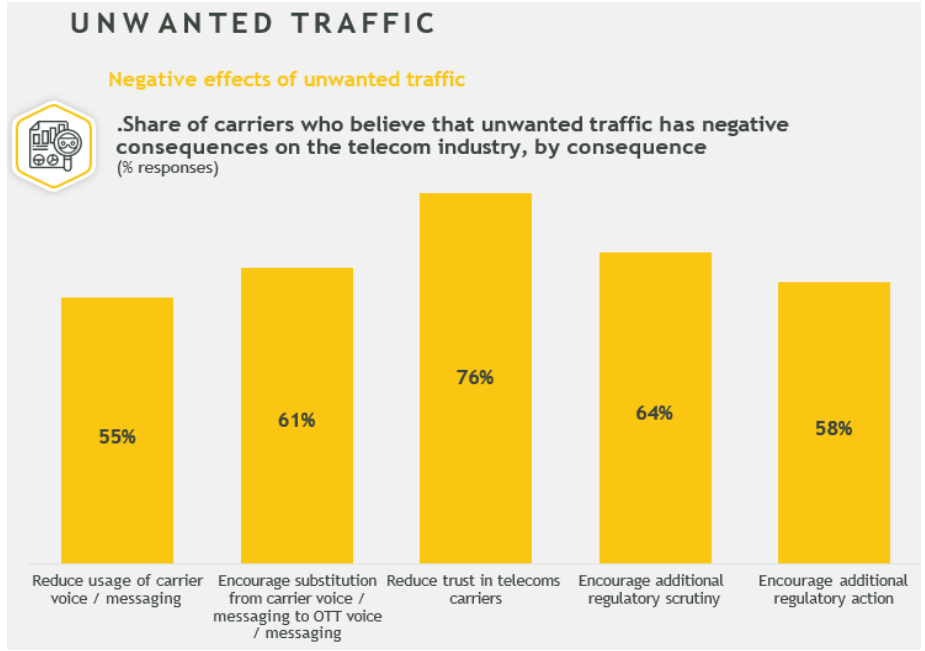
of carriers say unwanted traffic reduces trust in telecom carriers

**64%**

of carriers say unwanted traffic encourages additional regulatory scrutiny

**58%**

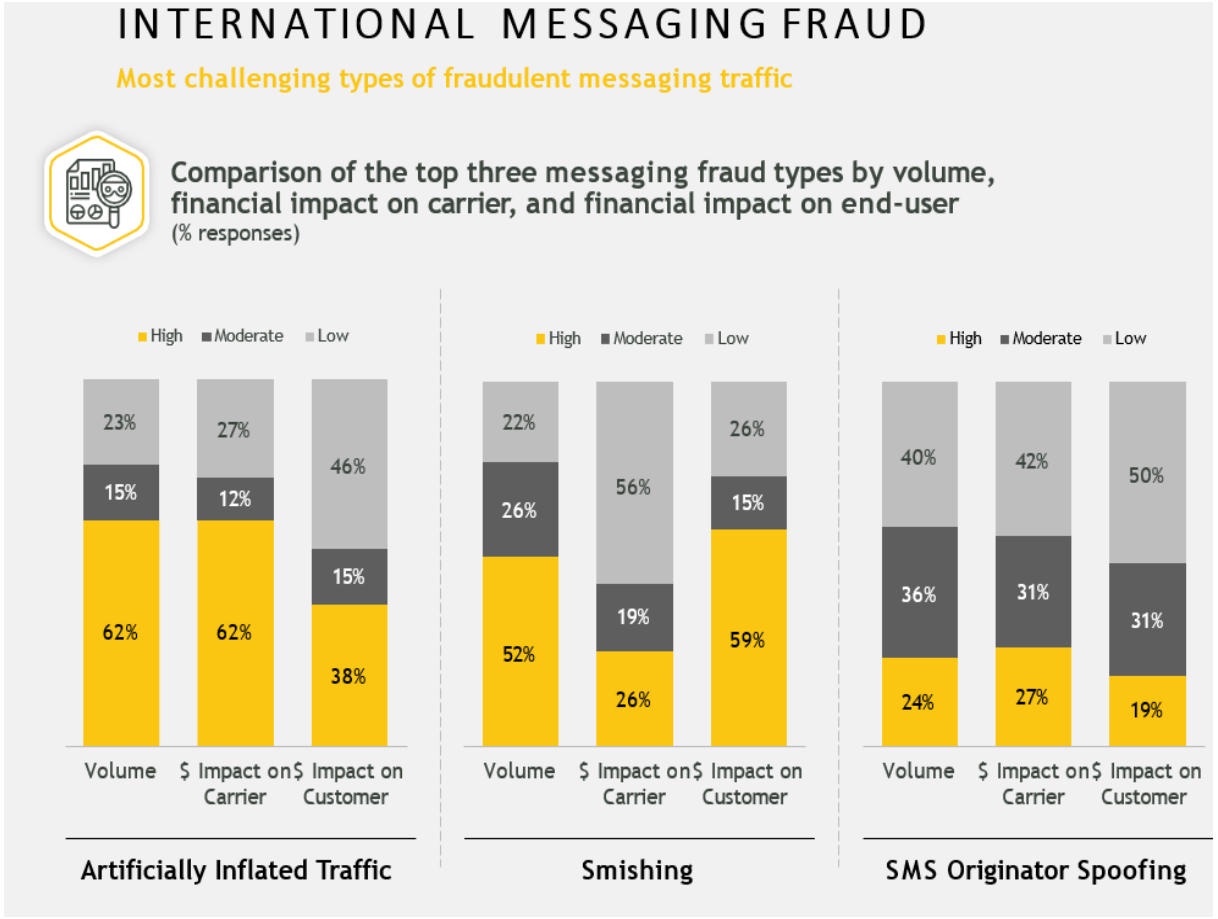
of carriers say unwanted traffic encourages additional regulatory action




Хуурамч ачаалал нь операторын орлого, нэр хүндэд болон зохицуулалтын орчинд эрсдэл дагуулж байна.

- **Итгэл сулруулах** – хэрэглэгчдийн **76%** нь операторт итгэл багассан гэж үзэж байна.
- **OTT рүү шилжих** – хэрэглэгчид Viber, WhatsApp зэрэг рүү шилжиж, орлого буурч байна **(61%).**
- **Хяналт, зохицуулалт нэмэгдэх** – хяналт чангарах (64%) ба шинэ арга хэмжээ авах шаардлага үүсэх (**58%).**
- **Үйлчилгээний ашиглалт буурах** – операторын дуудлага, мессежний хэрэглээ **55%**-иар буурч байна.

# ӨНӨӨГИЙН НӨХЦӨЛ БАЙДАЛ




AIT, Smishing and SMS Originator Spoofing are the biggest threats in terms of volume and financial impact

**62%**

of carriers say they have experienced a 'high' volume of Artificially Inflated Traffic (AIT)

**52%**

of carriers say they have experienced a 'high' volume of SMS phishing (Smishing)

**24%**

of carriers say they have experienced a 'high' volume of SMS Originator Spoofing

FTIDELTA GLF

•Ачааллын түвшин, Операторт үзүүлэх нөлөө , Хэрэглэгчид үзүүлэх нөлөө

**INTERNATIONAL MESSAGING FRAUD**

Мессежийн залилан нь өсөн нэмэгдэж буй асуудал бөгөөд **бизнесийн хувьд чухал энэ сувгийн** аюулгүй байдлыг хангах шаардлага улам бүр нэмэгдэж байна.

Мессеж залилангийн түгээмэл **гурван хэлбэр**:

**AIT (Artificially Inflated Traffic) –62%**

**Зохиомлоор өсгөсөн** мессежийн ачааллаас үүдэн операторуудад их хэмжээний нэмэлт зардал, **санхүүгийн эрсдэл** үүсгэдэг.

**Smishing–52%**

SMS мессеж ашиглан хэрэглэгчийг хуурч хувийн болон санхүүгийн мэдээлэл авах, эсвэл залилангийн **вэбсайт руу чиглүүлж** их хэмжээний **мөнгө** болон хувийн мэдээллээ **алдах**ад хүргэдэг.

**SMS Originator Spoofing– 24%**

Мессеж илгээгчийн нэр эсвэл дугаарыг хууль бусаар өөрчлөн, хүлээн авагчийг итгүүлэх арга. *Жишээ нь, банк, үйлчилгээний компаниас ирсэн мэт харагдана.*

**Шийдэл:** *Эрсдэлийг бууруулахын тулд операторууд **аюулгүй байдлын протокол**, хамгаалалтын шийдлээ тасралтгүй шинэчилж, сайжруулах*

# ӨНӨӨГИЙН НӨХЦӨЛ БАЙДАЛ

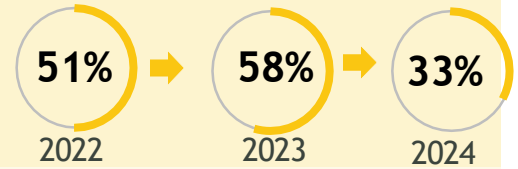
## THE IMPORTANCE OF FRAUDULENT TRAFFIC IN THE ORGANISATION

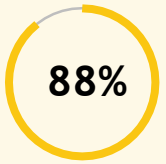


2024 онд carrier-уудын **64% нь** хуурамч ачааллын эсрэг тэмцэх нь "Нэн тэргүүний зорилт" гэж үзсэн залилантай тэмцэх зайлшгүй шаардлагатай байгааг харуулж байна.
Операторуудын дурдаж буй **гол шалтгаанууд:**

- Voice traffic, **ашиг буурч буй энэ үед** жижиг залилан ч ихээхэн санхүүгийн эрсдэл дагуулдаг тул урьдчилан сэргийлэх нь чухал.
- **AI, ML** зэрэг дэвшилтэт технологид тулгуурласан шинэ төрлийн залилан уламжлалт илрүүлэх системийн хамгаалалтыг даван гарах болсон тул байгууллагууд илүү хурдан, **уян хатан хамгаалалтын арга** хэмжээг нэвтрүүлэх шаардлагатай болж байна.

Үүний үр дүнд **'Бага ач холбогдолтой'** гэж үзсэн хариултын хувь буурсан




**Операторуудын 88% нь** залилангаас сэргийлэх нь **"Нэн тэргүүний зорилт"** гэж үзэж байна

# ЗАЛИЛАНГИЙН ЭСРЭГ БОДЛОГО, ЧИГ ХАНДЛАГА

## ЗАЛИЛАНГААС УРЬДЧИЛАН СЭРГИЙЛЭХ ОЛОН ТАЛТ САНААЧИЛГА

**Хиймэл оюун ухаан (AI) ба машин сургалтыг (ML) ашиглан бодит цагт залилан илрүүлж, блоклох нь гар ажиллагааг багасгаж, үр ашгийг нэмэгдүүлнэ**

*Хиймэл оюун ухаанд суурилсан аргачлал ашигласан бодит цагийн залилан илрүүлэх системд **хөрөнгө оруулж** байна. Энэ нь гар ажиллагаанд найдахгүйгээр залиланг шууд илрүүлж, бууруулах боломжийг олгодог..*

*Шинэ AI-д суурилсан залилангийн системүүд нь сэжигтэй traffic-ийг илрэнгүүт автоматаар блоклож, сүлжээнд хүрэхээс нь өмнө боломжит хохирлыг **урьдчилан зогсоохоор** бүтээгдсэн.*

**Салбар ба зохицуулагчтай хамтын ажиллагааг өргөжүүлж, мэдээлэл хуваалцсанаар дэлхийн залилан илрүүлэх хүчин чармайлт сайжирна.**

*Салбарын бүлгүүд болон гол түншүүдтэй идэвхтэй **хамтран ажиллаж**, залилан илрүүлэх чадвараа сайжруулж байна. **Өгөгдөл солилцож**, зохицуулагч байгууллагуудтай хамтран ажилласнаар залилангийн удирдлагын стратеги дэлхийн стандартад нийцэж байна.*

*Дэлхийн **форумуудтай** ойр хамтран ажилласнаар гарч буй шинэ төрлийн залилангийн аюулын талаар **мэдээлэлтэй байх** боломжтой болж байна. Энэ мэдлэгийн солилцоо нь илүү сайн бэлтгэлтэй, урьдчилан сэргийлэх хандлагатайгаар залилангийн эсрэг тэмцэхэд тусалж байна.*

**Реактив буюу дараа нь арга хэмжээ авах байдлаас урьдчилан таамаглалт шинжилгээнд суурилсан проактив хандлага руу шилжиж, илрүүлэлтийг ачаалал удирдлагын системд нэгтгэх**

*Идэвхтэй хүчин чармайлт гарган, реактив буюу **дараа нь арга хэмжээ авах хандлагаас** проактив буюу урьдчилан сэргийлэх арга барилд шилжиж, сэжигтэй үйл ажиллагаа **илрэнгүүт** залиланг блоклох дээр төвлөрч байна.*

***Шинэ хэрэгслүүд** (tool), системүүд нь сүлжээнд хүрэхээс нь өмнө залиланг **урьдчилан** таамаглаж, **сэргийлэх**ээр бүтээгдсэн. Залилан илрүүлэлтийг ерөнхий удирдлагад нэгтгэснээр бид санхүүгийн эрсдэл болон залилангаас үүдэх үйл ажиллагааны тасалдлыг бууруулж чадсан.*

Source: GLF Survey 2024.

# ЗАЛИЛАНГИЙН ЭСРЭГ БОДЛОГО, ЧИГ ХАНДЛАГА

## ХУУРАМЧ АЧААЛЛЫН ЭСРЭГ ЗОХИЦУУЛАЛТЫН АРГА ХЭМЖЭЭНИЙ ЖИШЭЭНҮҮД

Зохицуулагчид хууран мэхлэгчдээс гадна тэднийг зогсоох арга хэмжээ аваагүй телеком оператор, үйлчилгээ үзүүлэгчдэд шууд хариуцлага тооцох болсон бөгөөд хуурамч дуудлага, spam мессеж, өгөгдөл хамгаалалтын зөрчилд ногдуулах торгуулийн хэмжээ сая сая доллар, евро, фунт стерлингт хүрч, тогтмол өссөөр байна.

**Их Британи (2024):** Information Commissioner’s Office (ICO) нь **1.43 сая** хуурамч дуудлага хийсэн байгууллагуудад нийтдээ **£340,000-ын торгууль о**ногдуулжээ.

**Итали (2023):** Италийн зохицуулагч байгууллага **Garante** нь нэгэн мобайл оператор (MNO)-т телемаркетинг болон **robocall** зөрчил гаргасных нь төлөө **7.6 сая еврогийн торгууль** ногдуулжээ..

Энэ оператор нь хэрэглэгчийн өгөгдлийг буруу ашигласан бөгөөд маркетингийн дуудлагад зориулсан зөвшөөрлийг зохих ёсоор удирдаагүй нь **Европын Холбооны Өгөгдөл Хамгаалах Ерөнхий Журам (GDPR)**-ыг зөрчсөнд тооцогдсон байна

**Австрали (2023):**Australian Communications and Media Authority (ACMA) нь телекомын залилангийн эсрэг арга хэмжээгээ эрчимжүүлж, spam-ын эсрэг зохицуулалтыг зөрчсөн хэд хэдэн компанид торгууль ногдуулсан.

Жишээ нь, **Optus** компани нь spam болон robocalls зогсоож чадаагүйн улмаас **500,000 австрали долларын торгууль** хүлээжээ.

**Хятад (2023):** (Ministry of Public Security)-ны хэрэгжүүлсэн арга хэмжээнүүдийн үр дүнд **2.75 тэрбум** луйврын дуудлага, **2.28** тэрбум сэжигтэй SMS таслан зогсоогдож, **78,000 сэжигтэн** баривчлагдан, **210,000 гаруй хүнд захиргааны шийтгэл** ногдуулсан.

**АНУ (2024):** Federal Communications Commission-(FCC) нь хууль бус robocalls болон мессежийг чиглэсэн шинэ зохицуулалтыг зарласан байна. Шинэ журам нь операторуудаас **хууль бус дуудлагын урсгалыг хаах, VoIP-д хатуу хяналт тавих**ыг шаарддаг. Зөрчил гаргасан тохиолдолд **сая сая ам.долларын торгууль** ногдуулах зохицуулалттай.

# ЗАЛИЛАНГИЙН ЭСРЭГ БОДЛОГО, ЧИГ ХАНДЛАГА

## СИНГАПУР УЛСЫН ANTI-FRAUD ЗОХИЦУУЛАЛТЫН БОДЛОГО, ИНСТИТУЦИЙН АРГА ХЭМЖЭЭ:

**1. Технологид суурилсан хамгаалалт (IMDA-ийн арга хэмжээ)**

- **SMS Sender ID Registry (SSIR)** – зөвшөөрөгдсөн илгээгчийн ID-г албан ёсоор бүртгэж, бүртгэлгүй ID-г автоматаар “Likely-SCAM”-магадлалтай гэж тэмдэглэж анхааруулдаг.
- **Anti-scam фильтр ба блоклох механизм** – URL **(Uniform Resource Locator** буюу интернетийн вэб хаяг) бүхий сэжигтэй SMS, гадаад spoofing дуудлага, хүсээгүй контент бүхий мессежүүдийг шууд хаадаг.
- **SIM хэрэглээний зохицуулалт** – хэрэглэгчид олгох SIM картын тоог хязгаарласан (нэг хэрэглэгчид дээд тал нь 10 postpaid SIM).

Энэ нь **GSMA Open Gateway API +тархсан хамгаалалттай**

**2.Хамтарсан хариуцлагын тогтолцоо-** Shared Responsibility Framework **(SRF)**

2024 онд хэрэгжсэн SRF-ийн дагуу:

- **Банк, төлбөрийн үйлчилгээ үзүүлэгчид (FIs)** өндөр эрсдэлтэй үйлдэл дээр 12 цагийн cooling-off, real-time мэдэгдэл, “KILL SWITCH” **зогсоох** үйлчилгээ үзүүлэх үүрэгтэй.
- **Операторууд** зөвшөөрөгдөөгүй SMS илгээгчийн ID-г **блоклох**, scam URL-тэй SMS-ийг зогсоох, хэрэглэгчдэд урьдчилан анхааруулах үүрэгтэй.

Ингэснээр **scam-ын хохирлыг зөвхөн нэг тал хүлээх биш, банк ба оператор хамтран хариуцдаг “хамтарсан зохицуулалтын тогтолцоо”** бий болсон.

**3. Хууль эрх зүйн хүрээ**

•**Protection from Scams Bill (2025)** – онлайн болон уламжлалт залилангийн эсрэг шинэ хууль.

- Банк болон үйлчилгээ үзүүлэгчид scam сэжигтэй тохиолдолд **данс царцаах, мөнгө шилжүүлэлтийг зогсоох эрхтэй** болсон.
- **SIM картын буруу хэрэглээг** гэмт хэрэгт тооцдог болсон spoofing, залилан хийсэн тохиолдолд **эрүүгийн хариуцлага хүлээлгэнэ**.

Энэ нь **технологийн арга хэмжээ + хууль эрх зүйн зохицуулалт** уялдсан загвар юм.

**4. Институци**

- 2019 онд **Anti-Scam Centre** байгуулагдсан.
- 2021 онд **Anti-Scam Division**,
- 2022 онд **Anti-Scam Command (ASCom)** байгуулж, түсгай Scam Strike багууд ажиллаж эхэлсэн.
- Эдгээр нь **цагдаа, банк, телеком салбарын** хамтын ажиллагаатайгаар fraud илрүүлэх, мөрдөн шалгах**, таслан зогсоох үйл ажиллагаа** явуулдаг.

Энэ институцийн зохион байгуулалт нь **салбар хоорондын мэдээлэл солилцооны real-time channel** болж, cross-sector data sharing-ийг хэрэгжүүлж байна.

# ЗАЛИЛАНГИЙН ЭСРЭГ БОДЛОГО БА ШИЙДЛҮҮД

## МАЛАЙЗ УЛСЫН ANTI-FRAUD ЗОХИЦУУЛАЛТЫН БОДЛОГО, ИНСТИТУЦИЙН АРГА ХЭМЖЭЭ:

**1. Технологид суурилсан хамгаалалт**

**Telco Spam/Scam Filtering** – операторуудтай хамтран spam дуудлага, SMS-ийг блоклох системийг хэрэгжүүлсэн.

- **Контент устгал** – 2024 онд л гэхэд 66,507 **scam холбоотой контентыг устгасан**, 2025 оны эхний 2 сарын байдлаар 19,200 нэмэлт контент устгасан.
- **eKYC стандарт** – SIM бүртгэл, хэрэглэгчийн танилтыг хатуу мөрдөж, SIM картаар хийгдэх залилангийн эрсдлийг бууруулж байна.

Энэ нь GSMA Open Gateway-ийн **Number Verification, SIM Swap API**-ийн зарчимтай нийцэж байгаа технологийн хяналт юм.

**2. Салбар хоорондын хамтын ажиллагаа**

- **Securities Commission (SC) + MCMC** хамтарсан ажлын хэсэг (2025) онлайн scam эсрэг зохицуулалт, хэрэгжилт, AI ашиглан **контент устгал** чиглэлээр хүчтэй хамтын ажиллагаа эхлүүлсэн.
- **Bank Negara Malaysia (Төв банк)** болон **харилцаа холбооны** операторууд хамтран **phishing, fake account blocking** зэрэг арга хэмжээг авч байна.

Энэ нь **cross-sector antifraud ecosystem** - салбар хоорондын залилангийн эсрэг экосистем бий болгож байна.

**3. Хууль эрх зүйн хүрээ**

**Communications and Multimedia Act (CMA)** шинэчлэлт (2025):

- Fraud, spam, phishing зэрэг **зөрчлийг Section 233, 233A** дор тусгайлан гэмт хэрэгт тооцсон.
- Spam, unsolicited messages-ийг бүрэн хориглож, зөрчсөн үйлчилгээ үзүүлэгчдэд торгууль ногдуулдаг болсон.
- MCMC-д операторын үйлчилгээ зогсоох, аудит хийх эрх нэмэгдсэн.

**Licensing Guidebook (2025 шинэчлэлт)** – social media, messaging платформууд **(8 саяас дээш хэрэглэгчтэй)** заавал лиценз авах ёстой.Үүнд

- **Fraud, scam эсрэг хяналт, хэрэглэгчийн мэдээллийн хамгаалалт, deepfake/AI content хяналт** зэрэг нөхцөлүүдийг тусгасан.
- Зөрчсөн тохиолдолд ₨500,000 хүртэл торгууль, үйлчилгээ хаах эрхтэй.

Ингэснээр зөвхөн телеком биш, **OTT платформууд ч** хууль эрх зүйн antifraud **зохицуулалтад орсон.**

**4. Институцийн хүчин чадал**

- **MCMC** – телеком ба онлайн платформын үндсэн зохицуулагч.
- **SC (Securities Commission)** – хөрөнгө оруулагч, санхүүгийн салбарт antifraud зохицуулалт хэрэгжүүлдэг.
- **Bank Negara Malaysia** – KYC, eKYC болон санхүүгийн залилангийн хяналт.
- **Royal Malaysia Police (PDRM)** – enforcement болон cross-border мөрдөн шалгалт.

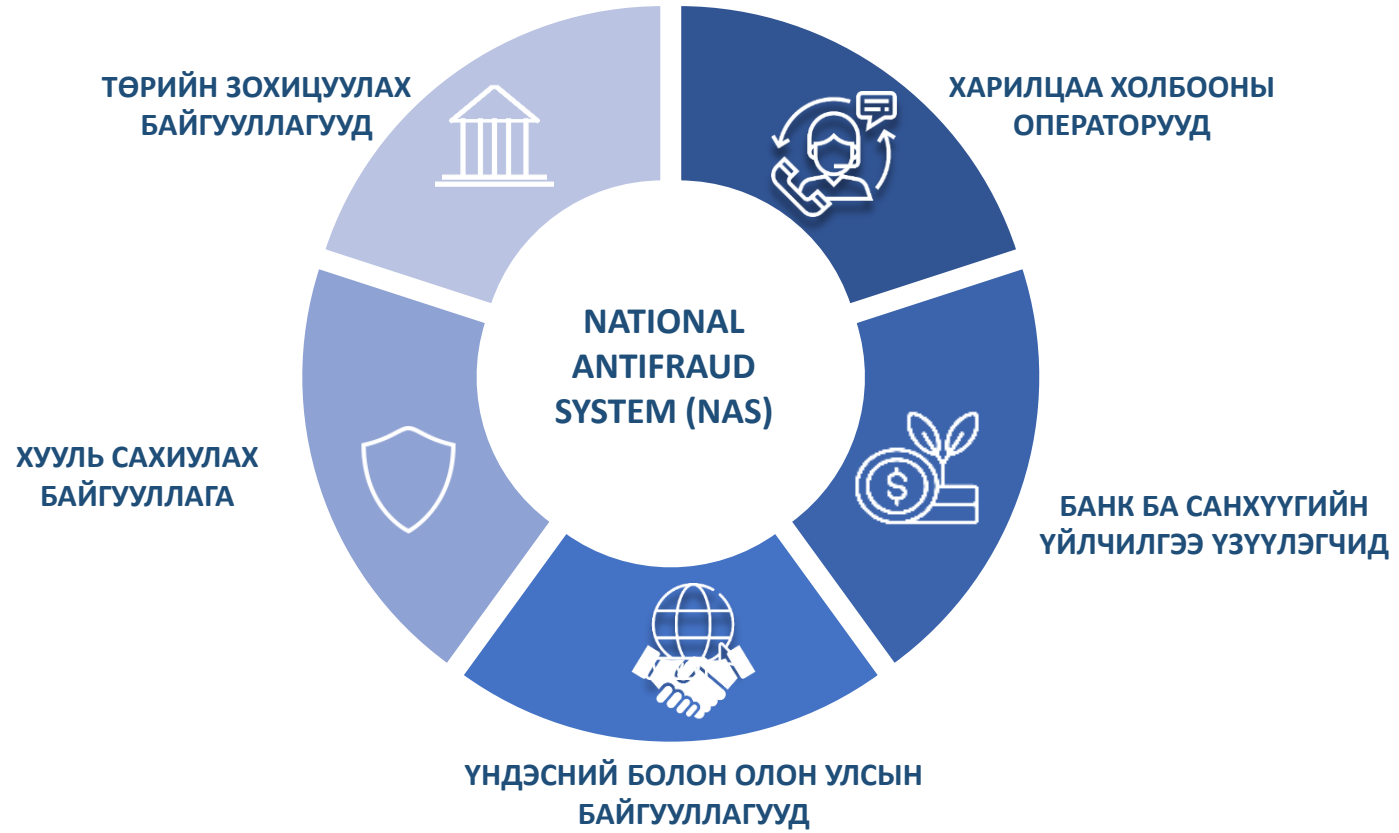
Институцийн хувьд **олон талт (multi-stakeholder) оролцогчидтой antifraud ecosystem** бий болсон.

# ЗАЛИЛАНГИЙН ЭСРЭГ ҮНДЭСНИЙ НЭГДСЭН СИСТЕМ

**National Anti-fraud System (NAS)** нь улс орны хэмжээнд телеком, санхүү, онлайн үйлчилгээ зэрэг олон салбарт үүсч буй **залилан**гийн үйлдлүүдийг илрүүлэх, урьдчилан **сэргийлэх**, зогсоох, мөрдөн шалгах, мэдээлэл солилцох нэгдсэн дэд бүтэц болон зохицуулалтын **цогц систем**ийг хэлнэ.

**NAS-д хамаарах гол оролцогч талууд:**

- ТӨРИЙН ЗОХИЦУУЛАХ БАЙГУУЛЛАГУУД
- ХАРИЛЦАА ХОЛБООНЫ ОПЕРАТОРУУД
- БАНК БА САНХҮҮГИЙН ҮЙЛЧИЛГЭЭ ҮЗҮҮЛЭГЧИД
- ХУУЛЬ САХИУЛАХ БАЙГУУЛЛАГУУД
- ҮНДЭСНИЙ БОЛОН ОЛОН УЛСЫН БАЙГУУЛЛАГА



# ЗАЛИЛАНГИЙН ЭСРЭГ ҮНДЭСНИЙ НЭГДСЭН СИСТЕМ

## NATIONAL ANTIFRAUD SYSTEM (NAS) -ИЙН ОРОЛЦОГЧ ТАЛУУД:

### ТӨРИЙН ЗОХИЦУУЛАХ БАЙГУУЛЛАГА

•**Харилцаа холбооны зохицуулагч байгууллага, Үндэсний кибер аюулгүй байдлын төв, Санхүүгийн зохицуулагч байгууллага** гэх мэт

***Үүрэг:*** хууль журмыг тогтоох, зохицуулах үүрэгтэй

### ХАРИЛЦАА ХОЛБООНЫ ҮЙЛЧИЛГЭЭ ҮЗҮҮЛЭГЧИД

**Мобайл операторууд** (MNO**), Суурин холбооны операторууд** (FNO), **Интернет үйлчилгээ үзүүлэгчид** (ISP)

***Үүрэг:*** *fraud эрсдлийн удирдлага, real- time бүртгэл, хяналт хийдэг*

### ҮНДЭСНИЙ БОЛОН ОЛОН УЛСЫН БАЙГУУЛЛАГУУД

**GSMA, ITU, CFCA, i3Forum,** APNI**, Үндэсний байгууллага**

***Үүрэг:*** *Cross-border fraud мэдээлэл, стандарт, best practice хуваалцах*

### БАНК БА САНХҮҮГИЙН ҮЙЛЧИЛГЭЭ ҮЗҮҮЛЭГЧИД

**Банк, финтек, төлбөрийн үйлчилгээ үзүүлэгчид**

***Үүрэг:*** *AML/KYC шалгалт хийх, эрсдлийг хянах, Залилангийн гүйлгээг илрүүлэх, OTP болон SMS banking мэдээлэл хуваалцах*

### ТӨРИЙН ЗОХИЦУУЛАХ БАЙГУУЛЛАГУУД

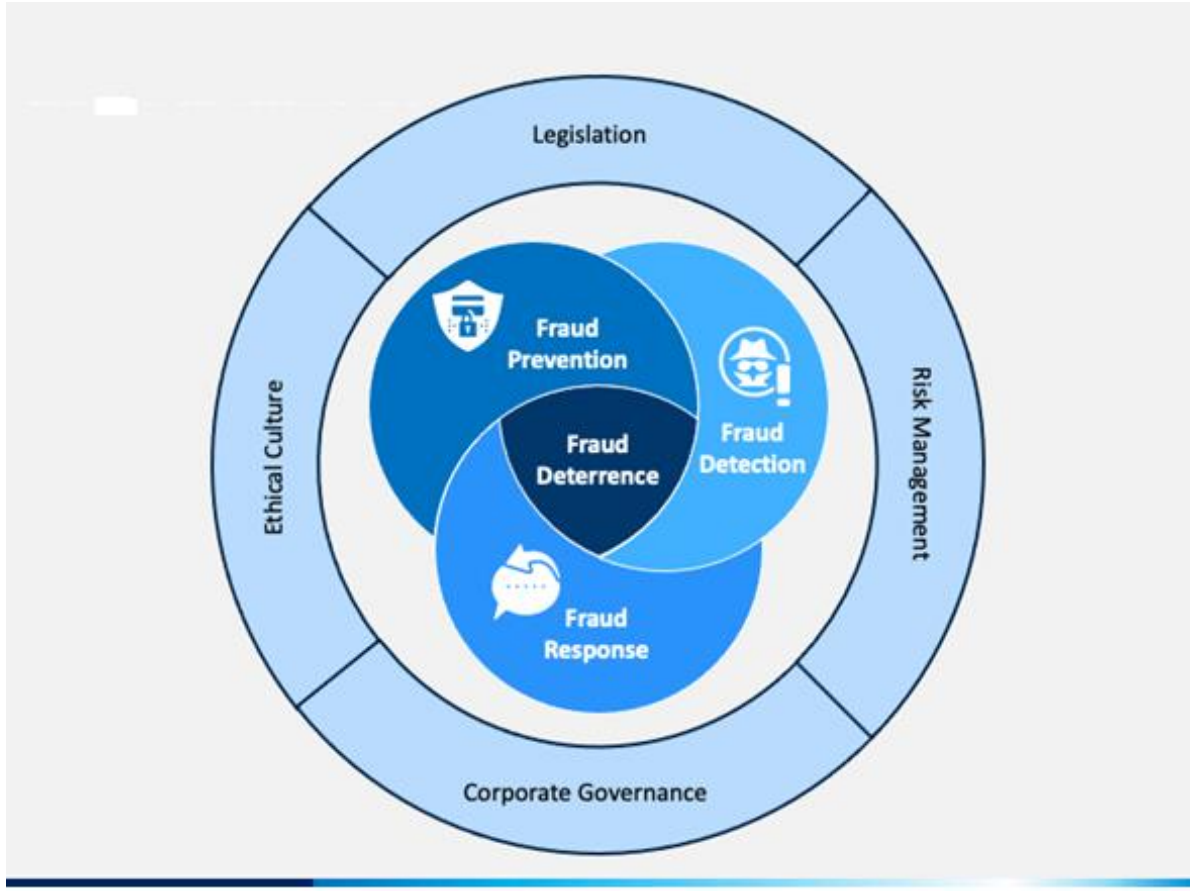
### ХУУЛЬ САХИУЛАХ БАЙГУУЛЛАГА

•**Цагдаа,Шүүх, прокурор**

***Үүрэг*****:** *Хэрэг шалгах, шийдэх, эрүүгийн болон иргэний хариуцлага хүлээлгэх*

# ЗАЛИЛАНГИЙН ЭСРЭГ ҮНДЭСНИЙ НЭГДСЭН ШИЙДЭЛ

## ANTI-FRAUD STRATEGY




**Anti-Fraud Strategy (залилангийн эсрэг стратеги)**-ийн үндсэн бүрэлдэхүүн:

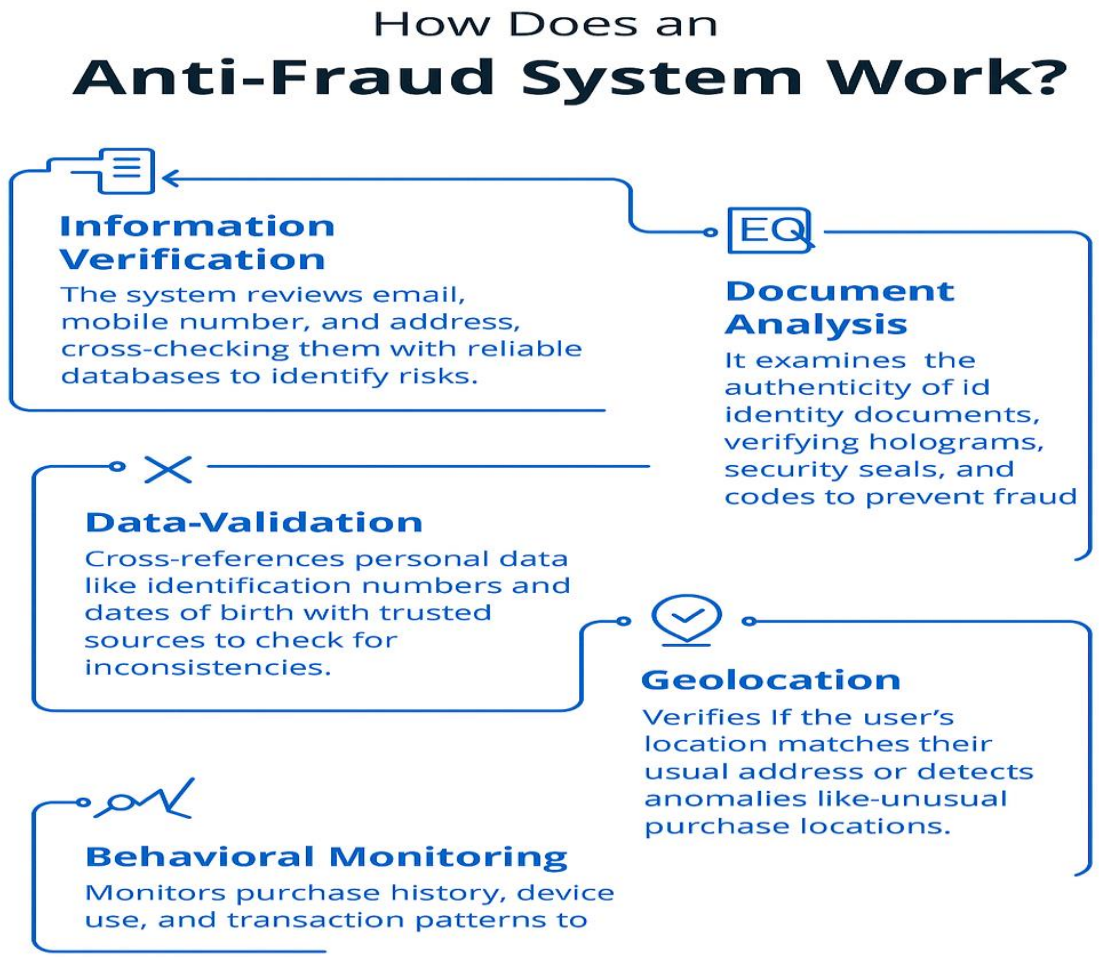
- **Fraud Prevention (Залилангаас урьдчилан сэргийлэлт)**
- **Fraud Detection (Залилан илрүүлэх)**
- **Fraud Response (Залилангийн эсрэг арга хэмжээ авах)**
- **Fraud Deterrence (Сэрэмжлүүлэх ба айлгах нөлөө)**

Эдгээр стратегиуд дараах **Гадаад хүчин зүйлсээр** дэмжигдэнэ:

- **Legislation (Хууль эрх зүй):** Залилангийн эсрэг хууль, журам.
- **Risk Management (Эрсдэл удирдлага):** Санхүү, үйл ажиллагааны эрсдэлийг тогтмол үнэлж бууруулах.
- **Corporate Governance (Корпорацийн засаглал):** Ил тод, хариуцлагатай байгууллагын засаглал.
- **Ethical Culture (Ёс зүйн соёл):** Ажилтан, хэрэглэгчдийн дунд шударга, ил тод зан үйлийг төлөвшүүлэх.

Дээрх үйл ажиллагаа нэгдэж хэрэгжсэнээр ирээдүйн залилан хийхийг бууруулах, хууль бус оролдлогоос урьдчилан сэргийлэх цогц тогтолцоо бүрддэг.

# ЗАЛИЛАНГИЙН ЭСРЭГ ҮНДЭСНИЙ НЭГДСЭН ШИЙДЭЛ




**Үндсэн бүрэлдэхүүн хэсгүүд:**

**Information Verification (Мэдээлэл баталгаажуулалт)**

- Хэрэглэгчийн имэйл, утасны дугаар, хаягийг шалгаж, итгэмжлэгдсэн мэдээллийн сантай тулган харьцуулна.
- Эрсдэлтэй буюу хуурамч мэдээллийг эрт илрүүлэх зорилготой.

**Document Analysis (Баримт бичгийн шинжилгээ)**

- Иргэний үнэмлэх, паспорт зэрэг баримтын жинхэнэ эсэхийг шалгана.
- Холограм, хамгаалалтын тэмдэг, QR/barcode зэрэг хамгаалалтыг баталгаажуулж, баримт хуурамч эсэхийг тодорхойлдог.

**Facial Recognition (Царай таних технологи)**

- Хэрэглэгчийн зураг болон баримт бичгийн зургыг харьцуулж ижил эсэхийг баталгаажуулна.
- Identity theft (хувийн мэдээллийн хулгай)-ийг багасгахад ашиглагдана.

**Data Validation (Өгөгдөл баталгаажуулалт)**

- Хувийн мэдээллийг (РД, төрсөн огноо гэх мэт) итгэмжлэгдсэн эх сурвалжтай тулган шалгана.
- Зөрүү, зөрчил илэрвэл систем анхааруулга өгнө.

**Geolocation (Байршлын шалгалт)**

- Хэрэглэгчийн байршил бүртгэлтэй хаягтай тохирч байгаа эсэхийг шалгана.
- Хэвийн бус худалдан авалт, үл мэдэгдэх улс/хот дахь гүйлгээг илрүүлнэ.

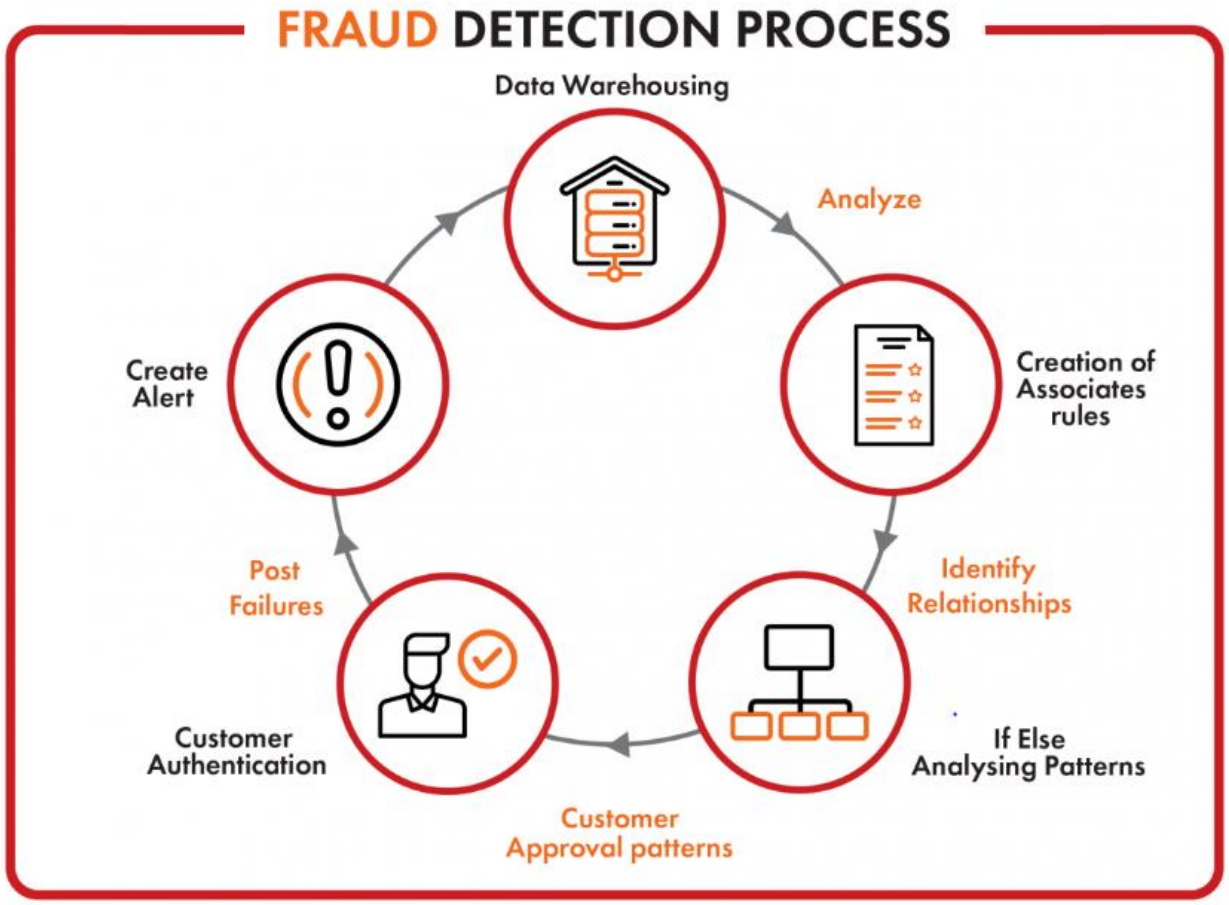
**Behavioral Monitoring (Зан төлөвийн хяналт)**

- Хэрэглэгчийн худалдан авалтын түүх, төхөөрөмжийн хэрэглээ, гүйлгээний хэв маягийг тасралтгүй хянадаг.
- Хэвийн бус эсвэл сэжигтэй үйлдэл илэрвэл сэрэмжлүүлэг үүсгэнэ.

Энэ систем нь **олон давхар хамгаалалттай anti-fraud экосистем** бөгөөд:

- Мэдээлэл болон баримтын үнэн зөвийг шалгах,
- Хувийн мэдээллийг баталгаажуулах,
- Байршил болон хэрэглэгчийн зан төлөвийг хянах замаар, **залилангийн оролдлогыг эрт илрүүлж, таслан зогсоох** зорилготой.

# ЗАЛИЛАНГИЙН ЭСРЭГ ҮНДЭСНИЙ НЭГДСЭН ШИЙДЭЛ




Энэ процесс нь **өгөгдөл цуглуулах → шинжлэх → дүрэм боловсруулах → холбоосуудыг илрүүлэх → хэрэглэгчийн зан төлөвтэй харьцуулах → баталгаажуулах → амжилтгүй оролдлогыг бүртгэх → сэрэмжлүүлэх** гэсэн **тасралтгүй мөчлөг** юм.

**Fraud Detection Process (Залилан илрүүлэх процесс)**-ийг үе шаттайгаар харуулсан тойрог схем юм.

**Үндсэн үе шатууд:**

**Data Warehousing (Өгөгдөл агуулах)**

- Бүх гүйлгээ, хэрэглэгчийн үйлдэл, системийн лог зэрэг өгөгдлийг цуглуулж, хадгалдаг.

**Analyze (Шинжилгээ хийх)**

- Өгөгдлийг задлан шинжилж, хэвийн болон хэвийн бус зан төлөвийг ялгаж авдаг.

**Creation of Associates Rules (Холбоо дүрэм боловсруулах)**

- Илрүүлэлтийн дүрэм, алгоритм боловсруулна (жишээ нь: тодорхой лимит давсан тохиолдолд сэрэмжлүүлэх).

**Identify Relationships (Холбоос тодорхойлох)**

- Гүйлгээ, хэрэглэгч, төхөөрөмж, байршлын хоорондын хамаарлыг илрүүлнэ.

**If Else Analyzing Patterns (Хэв маягт дүн шинжилгээ хийх)**

- “If-Else” логик ашиглаж, сэжигтэй хэв маягийг автоматаар ангилна.

**Customer Approval Patterns (Хэрэглэгчийн баталгаажуулалтын хэв маяг)**

- Хэрэглэгчийн ердийн үйлдэлтэй харьцуулж, сэжигтэй тохиолдлыг ялгана.

**Customer Authentication (Хэрэглэгчийн баталгаажуулалт)**

- Сэжигтэй гүйлгээ эсвэл үйлдлийг хэрэглэгчээр баталгаажуулах (OTP, KYC **2FA**-Two-Factor Authentication буюу хоёр шатлалтай баталгаажуулалт ).

**Post Failures (Амжилтгүй оролдлогын дараах хяналт)**

- Амжилтгүй болсон гүйлгээ, оролдлогыг бүртгэж, нэмэлт эрсдэл тооцоолол хийнэ.

**Create Alert (Сэрэмжлүүлэг үүсгэх)**

- Илэрсэн залилангийн магадлалтай үйлдлийг албан тушаалтанд мэдэгдэх эсвэл системээр блоклох.

# ЗАЛИЛАНГИЙН ЭСРЭГ ҮНДЭСНИЙ НЭГДСЭН СИСТЕМ

Харилцаа холбоо, санхүү, цахим орчинд тохиолддог залилангийн үйл ажиллагааг илрүүлэх, зогсоох, урьдчилан сэргийлэх зориулалттай **Anti-fraud системийн  түгээмэл хэрэгжүүлэлт:**

### 1. TELECOM ANTI-FRAUD SYSTEM

**Жишээ: GSMA FASG FS.11/FS.19-д суурилсан шийдлүүд**

- **CLI spoofing prevention** – дуудлагын эх сурвалжийг баталгаажуулж, хуурамч дуудлага (caller ID spoofing)-ыг тасалдуулна.
- **SIM box detection** – олон улсын дуудлагыг хууль бусаар орон нутгийн тарифаар дамжуулж буй SIM box-ыг илрүүлнэ.
- **Wangiri 2.0 blocking** – нэг хонх дуугараад тасардаг (callback fraud) залилангаас сэргийлнэ.
- **NRTRDE/TAP3 data analysis** – олон улсын роумингийн real-time дата дээр үндэслэн өндөр эрсдэлтэй хэрэглээг илрүүлнэ.

### 2. BANKING & FINTECH ANTI-FRAUD SYSTEM

**Жишээ: SAS Fraud Management, FICO Falcon, Oracle Financial Crime & Compliance**

- **Transaction Monitoring** – карт, шилжүүлэг, онлайн гүйлгээг real-time шинжилж, сэжигтэй үйлдлийг автоматаар зогсооно.
- **KYC & AML Integration** – хэрэглэгчийн таних баталгаажуулалт (eKYC), мөнгө угаахтай тэмцэх системтэй холбогдоно.
- **Machine Learning Scoring** – хэрэглэгчийн зан төлөвт дүн шинжилгээ хийж, хуурамч гүйлгээг оноогоор илрүүлнэ.

### 3. DIGITAL SERVICES / OTT ANTI-FRAUD

**Жишээ: Meta (Facebook) Security Systems, WhatsApp Fraud Detection, Google Play Protect**

- **Account Takeover Prevention** – OTP, 2FA ашиглан хэрэглэгчийн аккаунт булаах оролдлогоос хамгаална.
- **Spam & Phishing Detection** – AI/ML алгоритмаар мессеж, холбоос дээрх спам болон fishing оролдлогыг хаана.
- **Content Verification** – хэрэглэгчийн нийтлэл, зар, сурталчилгаа хууль бус эсэхийг автоматаар илрүүлнэ.

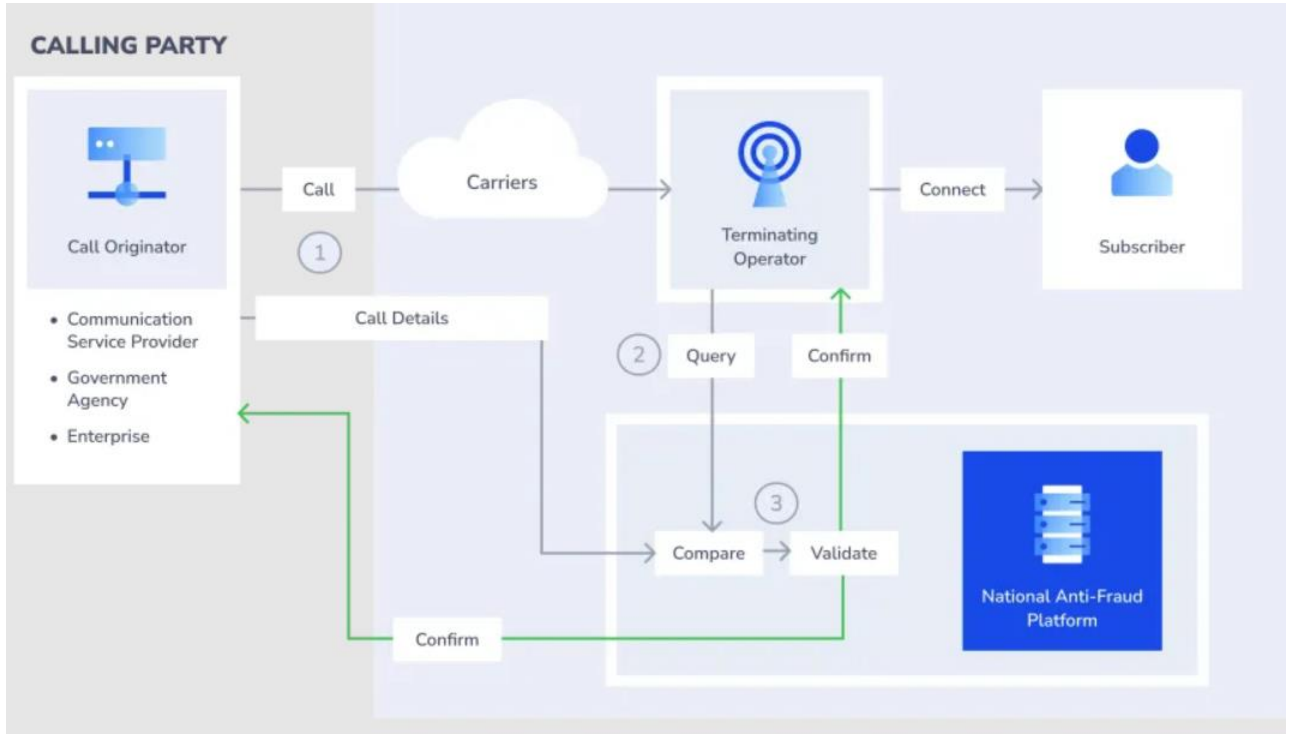
### 4. HYBRID NATIONAL ANTI-FRAUD PLATFORM

**Жишээ: UK “Scam Signal”, Malaysia’s National Scam Response Center (NSRC),**

- **Central Management Hub** – олон оператор, банк, финтек, төрийн байгууллагаас мэдээлэл цуглуулж, нэг цэгээс удирдана.
- **Cross-Sector Data Exchange** – телеком ↔ банк ↔ хууль сахиулагч байгууллагын хооронд өгөгдөл солилцоно.
- **Public Alerting** – хэрэглэгчдэд real-time scam alert илгээнэ (SMS, app push).

# ЗАЛИЛАНГИЙН ЭСРЭГ ҮНДЭСНИЙ НЭГДСЭН СИСТЕМ

## TELECOM - NATIONAL ANTI-FRAUD SYSTEM




**Үндэсний Anti-Fraud Платформ (NAFP-National Anti-Fraud Platform)**

**Зорилго:** Дуудлага, SMS-ийг холбогдохоос нь өмнө баталгаажуулж, spoof болон залилангийн урсгалыг хаах.

**Ажиллах зарчим:**

- Эх үүсвэрээс дуудлагын мэдээллийг NAFP-д илгээх
- Дуусах оператор баталгаажуулалтын хүсэлт илгээх
- NAFP эх үүсвэр ба дуусах операторын мэдээллийг тулгах
- Зөв бол дуудлагыг зөвшөөрөх, буруу бол залилан гэж тэмдэглэх
- Оператор блоклох, шошгожуулах, шалгах арга хэмжээ авах

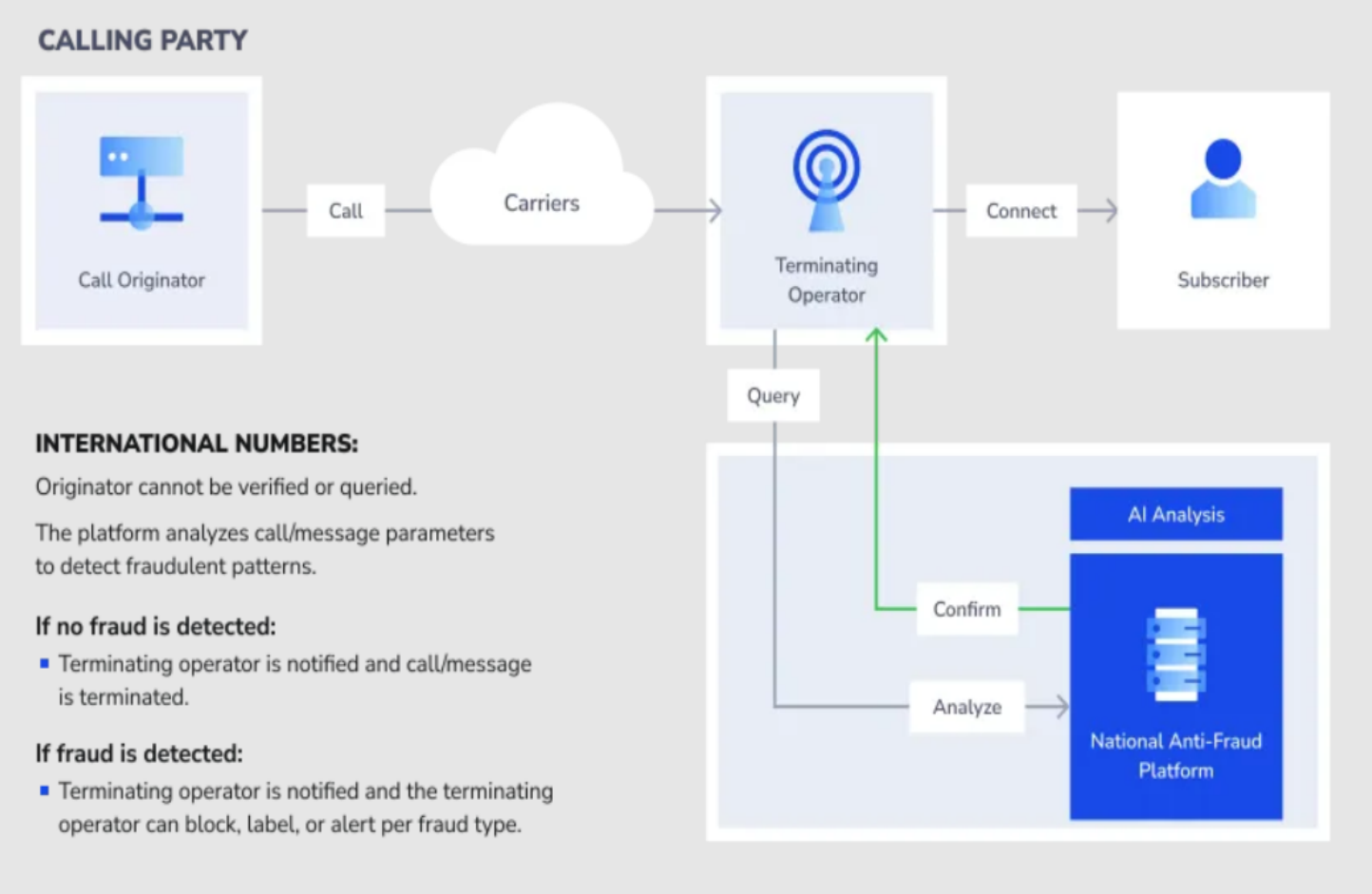
**Давуу тал:**

- Бодит цагийн out-of-band баталгаажуулалт
- Жинхэнэ урсгалыг баталгаажуулж false positive-ийг бууруулна
- Сүлжээн дэх итгэлийг сэргээж, хэрэглэгч, оператор, аж ахуйн нэгжийг хамгаална

**Үндэсний түвшинд хэрэгжүүлбэл spoof хийсэн дуудлага, SMS-ийг 100% зогсооно.**

# ЗАЛИЛАНГИЙН ЭСРЭГ ҮНДЭСНИЙ НЭГДСЭН СИСТЕМ

## TELECOM ANTI-FRAUD SYSTEM- AI-Powered Fraud Detection -AB Handshake




**NAFP (National Anti-Fraud Platform) – Хиймэл оюунд суурилсан залилан илрүүлэлт (AI-Powered Fraud Detection)**

**Зорилго:** End-to-End баталгаажуулалтаас зугтах олон улсын болон дотоодын жинхэнэ дугаар ашигласан нарийн залилан илрүүлэх.

**Давуу тал:**

- Илүү ухаалаг (adaptive learning),
- Илүү өргөн (cross-channel),
- Илүү хурдан (real-time at scale),
- Илүү үр дүнтэй (low FPR + fund tracing) байдгаараа онцлог

**Илрүүлэх залилан:** IRSF, Wangiri 2.0, AIT, Smishing/Vishing, PBX hacking, Flash calls, SIM box, CLI spoofing, Spam/Robocall, A2P bypass гэх мэт.

**Интеграц ба өргөтгөх чадвар:** SIP, Diameter, HTTP API, ISUP протоколуудыг дэмжинэ. Legacy-гээс 5G/6G хүртэл нийцтэй. 2–3 сард үндэсний хэмжээнд нэвтрүүлэх боломжтой.

Энэ нь зөвхөн нэг байгууллага бус, бүхэлдээ **үндэсний хэмжээнд интеграцлагдсан antifraud экосистем** болж чаддаг.

## TELECOM ANTI-FRAUD SYSTEM

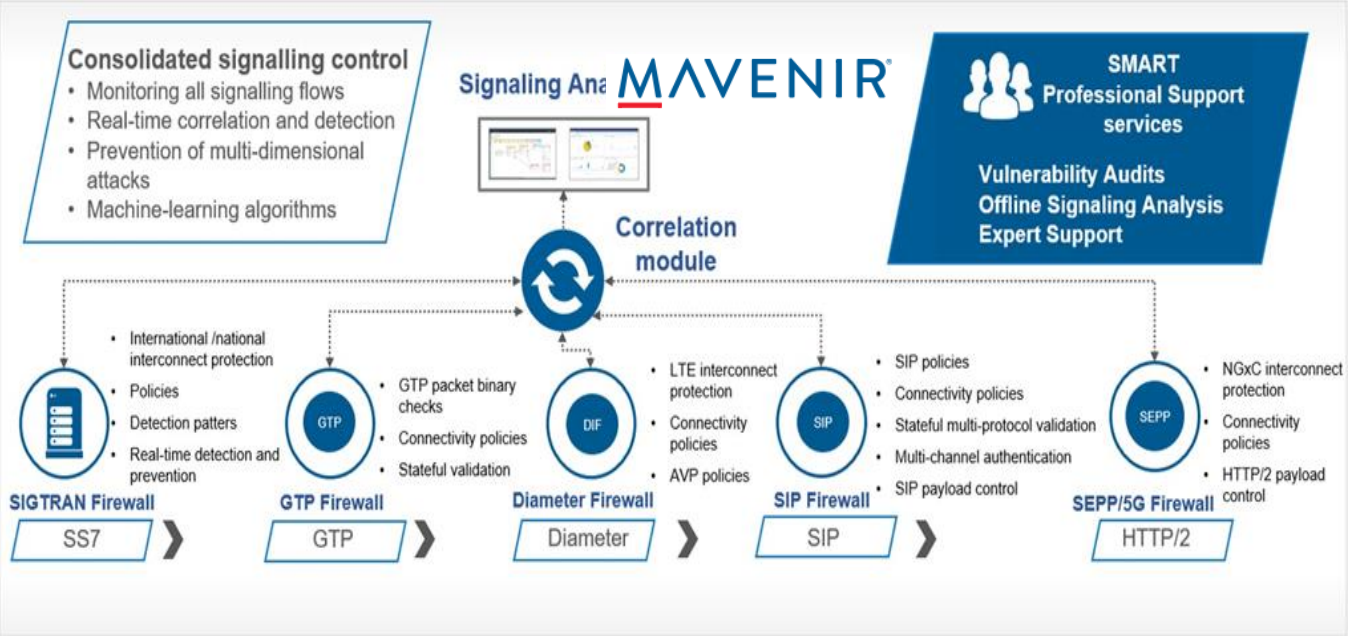
| Элемент / Шийдэл | Үүрэг / Онцлог |
|---|---|
| Signaling Firewall | SS7 болон Diameter traffic real-time хамгаалалт (+ SIP, GTP-C, HTTP/2) |
| Monitoring & Analytics | Fraud дүн шинжилгээ, alerts, reporting |
| Threat Intelligence Feed | **GSMA FASG-аас ирэх FS.11 / FS.19 хүрээнд шинэ аюулын мэдээллийн удирдлага** |
| Deployment Styles | Inline, Overlay, Integrated загваруудын сонголттой |
| Жишээ Шийдлүүд | Titan.ium, Enea, NetNumber, F5, Mavenir зэрэг industry-leading platform-ууд |

**GSMA-ЫН FS.11 (SS7) БОЛОН FS.19 (DIAMETER)** нь MNO-үүдэд дагах ёстой anti-fraud аргачлалуудыг тогтоож өгдөг бөгөөд эдгээрийн дагуу боловсруулах **FIREWALL АРХИТЕКТУРУУД** нь сүлжээг хамгаалах үндсэн хэлхээ болдог.
Real-time monitoring, cross-protocol correlation, ML-д суурилсан шинжилгээ болон flexible deployment архитектурууд нь өнөөгийн modern мобайл сүлжээний аюулгүй байдлын суурь гэж хэлж болно.

# ЗАЛИЛАНГИЙН ЭСРЭГ ҮНДЭСНИЙ НЭГДСЭН СИСТЕМ

**NETNUMBER Signaling Firewall (TITAN платформ)**

- FS.11 болон FS.19 стандарттай нийцсэн **multi-protocol signaling firewall** шийдэл.
- SS7 болон Diameter траффикт real-time inspection хийж, хортой “UpdateLocation” мессежүүдийг блоконо.
- Carrier-grade бүтэцтэй тул STP/HSS зэрэг гол сүлжээ дотроо inline байршуулдаг



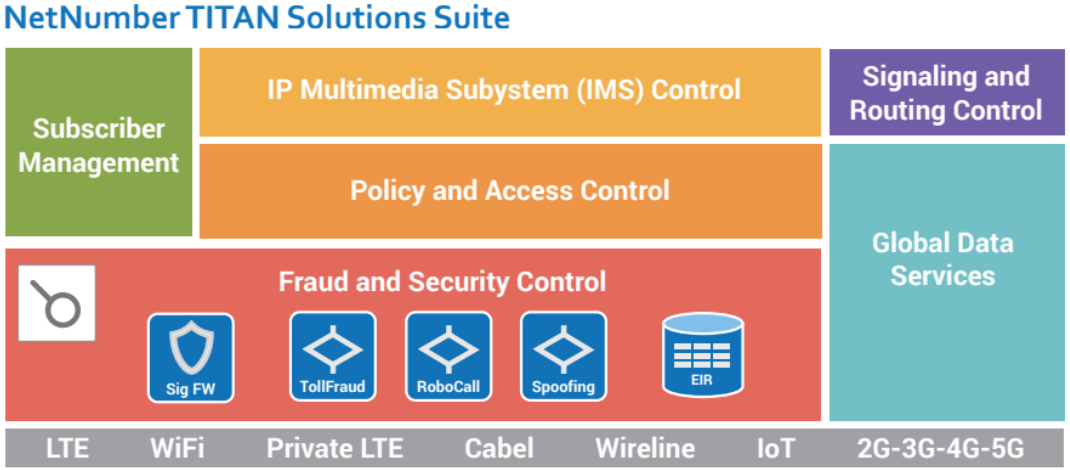
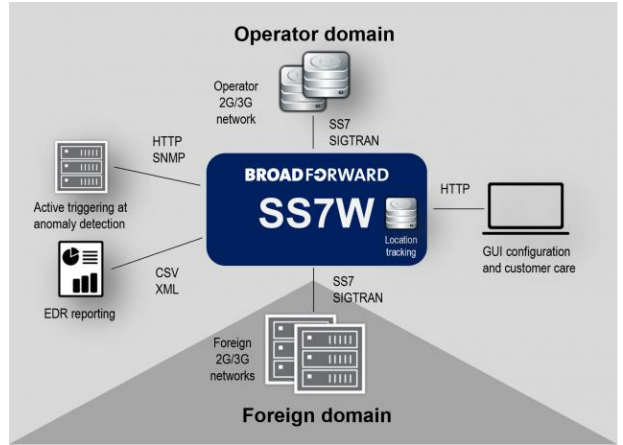




*Figure 1 – NetNumber TITAN Solutions Suite with focus on Security and Fraud Mitigation applications*

**MAVENIR Signaling Firewall**

- FS.11 болон FS.19 стандартад нийцсэн, уламжлалт дүрэмд суурилсан (rule-based) firewall ажиллагаар **машин сургалт (Machine Learning)**-тай хослуулсан ухаалаг хамгаалалтын шийдэл.
- DoS, eavesdrop, SMS interception,location tracking гэх мэт олон төрлийн аюулыг илрүүлдэг




**BROADFORWARD SS7FW болон Diameter Firewall**

•**SS7FW** нь FS.11-ийн ангилалд нийцэх firewall :

- **Velocity check** ашиглаж “time-distance plausibility” хангах (хамгийн хурдацтай байршлын өөрчлөлт)
- “Transparent mode” – шинэ дүрмийг туршиж, алдаагүй баталгаажуулж байж live system-д нэвтрүүлэх.

•**Diameter Firewall (DFW)** нь FS.19-д нийцэх юм:

- Уламжлалт биш, динамик дүрмүүдийг GUI-аар удирдах боломжтой
- SS7FW-тай хослуулан хэрэглэх боломжтой.

# ЗАЛИЛАНГИЙН ЭСРЭГ ҮНДЭСНИЙ НЭГДСЭН СИСТЕМ

## BANKING & FINTECH ANTIFRAUD SYSTEM


**Banking & Fintech Anti-fraud System** нь:

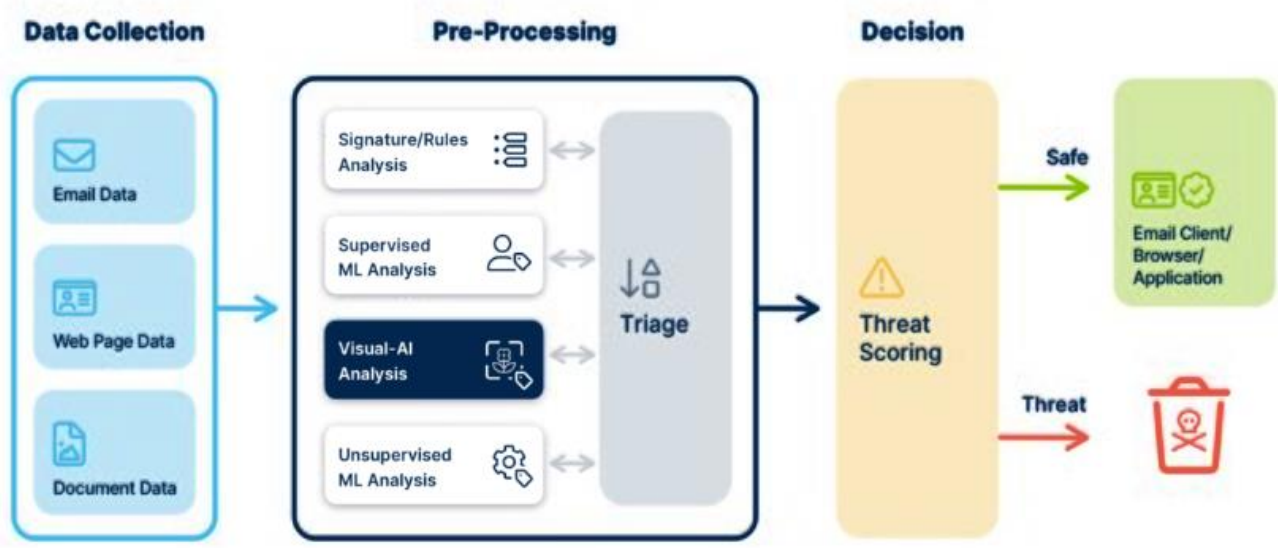
- **Fraud Management (залилангийн илрүүлэлт)**
- **Fraud Framework (салбар бүрт тохирсон шийдэл)**
- **AML (мөнгө угаахтай тэмцэх)**
- **Case Management (хэргийг удирдах ба шалгах)**

гэсэн **дөрвөн үндсэн тулгууртай** бөгөөд банк, финтек болон бусад салбарт залилан, мөнгө угаах эрсдэлийг бууруулах **нэгдсэн antifraud экосистем**ийг бий болгодог.

**SAS-ийн anti-fraud платформ** нь **Integrated Analytics & Case Investigation** буюу **нэгдсэн өгөгдлийн шинжилгээ + кейсийн мөрдөн шалгалт** дээр тулгуурладаг.

# ЗАЛИЛАНГИЙН ЭСРЭГ ҮНДЭСНИЙ НЭГДСЭН СИСТЕМ

## DIGITAL SERVICES / OTT ANTI-FRAUD




Энэ архитектур нь **имэйл, веб, баримт зэрэг олон төрлийн дижитал өгөгдөл дээр anti-fraud илрүүлэлт хийх** процессийг шат дараатайгаар харуулж байна:

- Өгөгдөл цуглуулах →
- AI/ML ба дүрмийн анализ хийх →
- Эрсдэлийн оноо өгөх →
- Хэрэглэгчид аюулгүй өгөгдлийг хүргэх, залилангийн эрсдэлийг устгах.

Энэ схемийг OTT anti-fraud платформд хэрэглэж болох ба **Account Takeover Prevention, Spam/Phishing Detection, Content Verification** модулиудыг  ийм урсгалд тааруулж хөгжүүлдэг.

# ЗАЛИЛАНГИЙН ЭСРЭГ ҮНДЭСНИЙ НЭГДСЭН СИСТЕМ

NAS-ийн архитектур нь **GSMA (телеком fraud API ба мэдээлэл солилцоо) + ITU (сүлжээ, кибер аюулгүй байдал) + ISO (эрсдэл, аюулгүй байдал, авлигын эсрэг, мэдээлэгчийн хамгаалалт)** гэсэн олон улсын **түлхүүр стандартуудын нэгдсэн экосистем** дээр тулгуурладаг.

**GSMA (Mobile & Telecom Fraud Prevention Standards)**

**•GSMA FASG (Fraud and Security Group):**
- CLI spoofing, SMS phishing, IRSF зэрэг телеком залилангийн эсрэг удирдамж.
- Fraud Intelligence Sharing Hub (T-ISAC) – операторуудын хооронд мэдээлэл хуваалцах.

**•GSMA Open Gateway API:**
- **Number Verification** – хэрэглэгчийн дугаарын бодит баталгаажуулалт.
- **SIM Swap Detection** – SIM солилцох залиланг илрүүлэх.
- **KYC Match** – хэрэглэгчийн мэдээллийг баталгаажуулах.

**ITU (International Telecommunication Union Standards)**

**•ITU-T X.805** – Сүлжээний end-to-end аюулгүй байдлын архитектур.
**•ITU-T X.1060** – Ubiquitous networks-ийн аюулгүй байдлын хүрээ.
**•ITU Cybersecurity Guidelines** – cross-border fraud болон кибер гэмт хэргээс хамгаалах удирдамж.
**•CERT Integration** – Үндэсний болон олон улсын CERT-тэй мэдээлэл солилцох тогтолцоо.

**ISO (International Organization for Standardization Standards)**

**•ISO/IEC 27000 цуврал:**
- Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо (ISMS).
- ISO/IEC 27032 – Кибер орчны аюулгүй байдлын удирдамж.

**•ISO 31000** – Эрсдэлийн удирдлагын тогтолцоо.
**•ISO 37001** – Авлигын эсрэг удирдлагын тогтолцоо.
**•ISO 37002** – Мэдээлэгчийн (whistleblower) хамгаалалтын тогтолцоо.
**•ISO 22301** – Бизнесийн тасралтгүй ажиллагааны удирдлага.

**NAS-ийн олон улсын нийцлийн зарчим**

**•Data & Security:** ISO 27000, ITU X.1060, GSMA Open Gateway API.
**•Fraud Detection & Risk Management:** GSMA FASG guidance, ISO 31000.
**•Case Management & Governance:** ISO 37001, ISO 37002, ITU X.805.
**•Collaboration & Interoperability:** GSMA T-ISAC, ITU frameworks, Europol/Interpol info-sharing.
**•Business Continuity & Resilience:** ISO 22301.

# ЗАЛИЛАНГИЙН ЭСРЭГ ҮНДЭСНИЙ НЭГДСЭН СИСТЕМ

Олон улсын практик дээр үндэслэсэн C**ustomized architecture** layer

| Давхарга | Гол бүрэлдэхүүн | Үүрэг / Функц |
|---|---|---|
| **1. Access Layer (Хандалтын түвшин)** | - Subscriber authentication (SIM/eSIM, device ID)<br>- KYC/ID баталгаажуулалт<br>- Number Verification API<br>- MFA/OTP | Хэрэглэгчийн оролтыг баталгаажуулах, зөвшөөрөл олгох |
| **2. Network/Core Layer (Үндсэн сүлжээ)** | - Telecom core (IMS/VoIP, SS7/Diameter)<br>- SMSC, MSC/VMSC<br>- Fraud firewalls (SMS, SS7, SIP)<br>- Banking core (RTGS, Card switch, AML engine) | Үндсэн сүлжээнд залилан илрүүлэх ба блоклох (CLI spoofing, SIM swap, transaction fraud) |
| **3. Data Layer (Өгөгдлийн давхарга)** | - Central antifraud data lake<br>- Data integration (telecom, bank, fintech, govt DBs)<br>- Data governance & quality controls | Олон эх сурвалжийн өгөгдлийг нэгтгэж, шинжилгээнд бэлтгэх |
| **4. Analytics & Detection Layer (Шинжилгээ ба илрүүлэлт)** | - AI/ML fraud detection engine<br>- Predictive & anomaly analytics<br>- Real-time monitoring (≤500ms) | Хэвийн бус үйлдэл, өндөр эрсдэлтэй гүйлгээ/дуудлагыг илрүүлэх |
| **5. Service/Application Layer (Үйлчилгээний түвшин)** | - Case management system<br>- Fraud reporting portals<br>- Customer alert services (fraud warnings)<br>- Whistleblower protection | Илрүүлсэн кейсүүдийг удирдах, хэрэглэгчид мэдээлэх, гомдол авах |
| **6. Governance & Coordination Layer (Засаглал ба зохицуулалт)** | - National regulator, FIU integration<br>- CERT/CSIRT холбоос<br>- Cross-border sharing (Europol, Interpol, GSMA T-ISAC) | Зохицуулалт, олон улсын хамтын ажиллагаа, хууль эрх зүйн мөрдлөг |
| **7. Security & Compliance Layer (Нэвт хэрэгжих хамгаалалт)** | - ISO/IEC 27000 (info security)<br>- ISO 31000 (risk management)<br>- ISO 37001/37002 (anti-bribery, whistleblowing)<br>- ITU-T X.805 (E2E security) | Бүх давхаргад нэвт үйлчлэх мэдээллийн аюулгүй байдал ба нийцэл |

**End-to-End Security Architecture ITU-T X.805:**
Сүлжээний аюулгүй байдлын **архитектурын загвар :**

- **8 хамгаалалтын хэмжээстэй**
- **3 давхаргын хамгаалалттай** (infrastructure, services, applications).

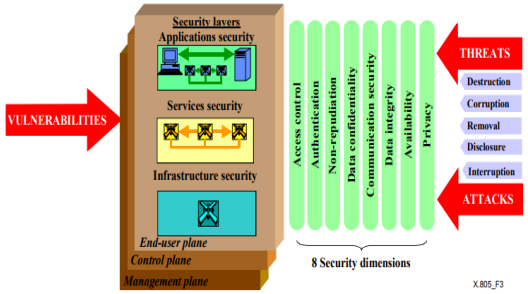



Figure 3/X.805 – Security architecture for end-to-end network security

**TS 33.501**-ийн стандарт нь:

- **Cross-operator мэдээлэл солилцоо аюулгүй** байх
- Fraud detection-д ашиглагдах SMS, OTP, call data integrity-г хамгаалах
- IMSI, MSISDN зэрэг хувийн мэдээллийн нууцлалыг хангах

**ETSI TS 103 645 стандарт**

- IoT төхөөрөмжийн **default password-ийг хориглох**
- **Аюулгүй програм хангамжийн шинэчлэлт**ийг хангах
- **Мэдээлэл устгах/засварлах боломж** олгох
- **Хувийн мэдээллийг хамгаалах**
- **Эрсдэлийн удирдлагын аргачлал** нэвтрүүлэх зэрэг шаардлагууд багтсан.

## NAS СҮЛЖЭЭНИЙ ПРОТОКОЛ

| Салбар | Ашиглах протокол | Үндсэн зориулалт / Үүрэг |
|---|---|---|
| **Telecom** | SS7 / SIGTRAN (MAP, CAP, INAP) | Дуудлага, SMS дохиолол дамжуулах, CLI spoofing, SIM swap илрүүлэх |
| | SIP / Diameter / IMS | VoIP, LTE/5G орчинд дугаар баталгаажуулалт, STIR/SHAKEN хэрэгжүүлэх |
| | GSMA Open Gateway APIs (REST/HTTPS) | Number Verification, SIM Swap Detection, KYC Match |
| **Bank & Fintech** | ISO 20022 / SWIFT | Санхүүгийн гүйлгээний мессеж, real-time fraud scoring |
| | Open Banking APIs (REST/JSON) | Хэрэглэгчийн дансны баталгаажуулалт, transaction monitoring |
| | AML/Fraud APIs | Санхүүгийн зөрчил илрүүлэх, сэжигтэй гүйлгээ (STR/CTR) илгээх |
| **Government / Regulator** | SOAP / REST Secure Web Services | Case management, тайлан, зохицуулалтын дата солилцоо |
| | FIU Reporting Protocols | Сэжигтэй гүйлгээний тайлан (STR/CTR) дамжуулах |
| **Cybersecurity / CERT** | Threat intelligence sharing protocols (STIX/TAXII) | Scam URL, phishing, malware, кибер халдлагын IOC солилцох |
| **International Cooperation** | Interpol/Europol data exchange standards | Cross-border fraud intelligence sharing |
| | GSMA T-ISAC sharing feeds | Олон улсын телеком операторуудын fraud мэдээлэл солилцоо |

**GSMA FASG -Fraud and Security Group Guidelines:**

**CLI Spoofing хамгаалалт**

- **STIR/SHAKEN framework** (caller ID authentication, USA & GSMA стандарт).
- **Call Scoring & Anomaly Detection** – NAS дээр дуудлагын хэв маягийг анализ хийх.
- Operator-to-operator verification protocols

**Wangiri хамгаалалт**

- **Call pattern analysis** – богино дуудлага, олон удаа давтагдсан дуудлагыг NAS хянах.
- **Blacklist / Greylist** – эрсдэлтэй дугаарыг автомат блоклох.
- Subscriber education – scam дуудлагаас сэрэмжлүүлэх.

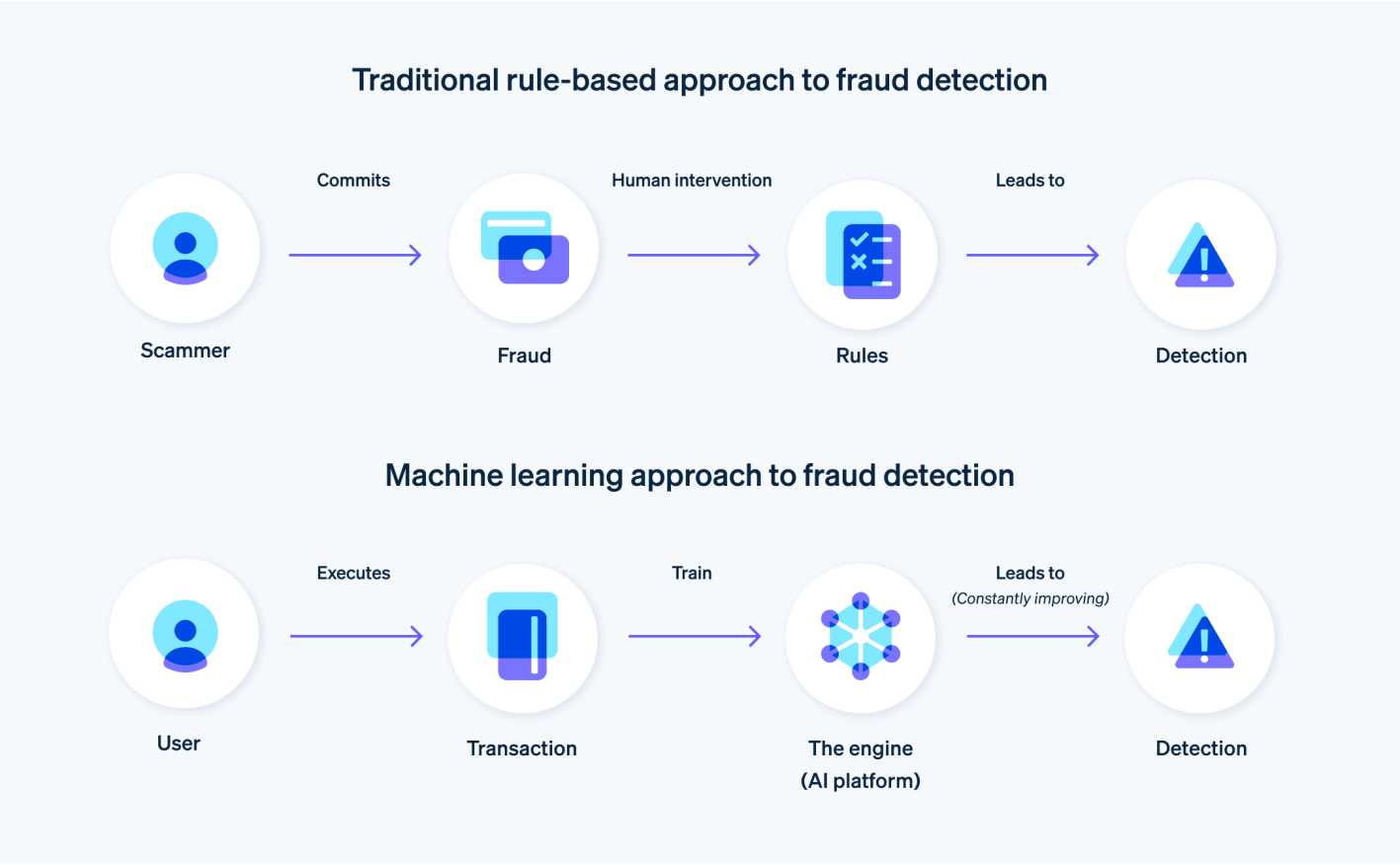
**IRSF (International Revenue Share Fraud) хамгаалалт**

- **Call routing monitoring** – NAS операторoор дамжиж буй олон улсын дуудлагын төлбөрийг хянах.
- **High-risk destination flagging** – IRSF-д өртөмтгий улсууд, дугаарууудыг тэмдэглэх.
- **Threshold alerts** – abnormal call volume / revenue exceed-т мэдэгдэх.

**NAS СИСТЕМД ХЭРЭГЖҮҮЛЭХ АРГА**

- CLI spoofing, Wangiri, IRSF detection & mitigation modules интеграци хийх.
- Cross-operator monitoring: Fraud-д өртсөн дугаарыг бусад оператортой share хийх.
- GSMA FASG guidelines-д нийцсэн **audit & reporting**-ийг хийх.

# ЗАЛИЛАНГИЙН ЭСРЭГ ҮНДЭСНИЙ НЭГДСЭН ШИЙДЭЛ




## Залилан (fraud) илрүүлэх арга барил

**Уламжлалт дүрэмд суурилсан арга (Rule-based approach)**:
**Scammer (залилан хийх этгээд)** → Залилан үйлдэнэ.
•**Fraud (залилангийн үйлдэл)** → илрэхийн тулд хүн оролцож дүрэм зохионо.
•**Rules (дүрэм)** → гар аргаар тогтоосон нөхцөлүүд (жишээ: нэг дор олон гүйлгээ хийсэн бол сэжигтэй, эсвэл тодорхой дүнгээс давсан бол шалгах гэх мэт).
•**Detection (илрүүлэлт)** → **зөвхөн тухайн дүрмэнд таарсан тохиолдолд илрүүлдэг.**
Шинэ төрлийн залилан гарвал дүрэм шинэчлэгдтэл илрүүлэхгүй. Уян хатан бус, хүний оролцоо их.

**Машин сургалт (Machine Learning approach)**:
•**User (хэрэглэгч)** → гүйлгээ хийнэ.
•**Transaction (гүйлгээний өгөгдөл)** → AI системд орно.
•**The engine (AI platform)** → хиймэл оюун өөрөө сургалт хийж, гүйлгээний хэв маяг, зан төлөвийг танина.
•**Detection (илрүүлэлт)** → AI тогтмол суралцаж, **шинэ залилангийн аргыг ч хурдан илрүүлдэг.**
Өгөгдөл дээр үндэслэн тасралтгүй сайжирна, шинэ төрлийн залиланг дүрэм шинэчлүүлэхгүйгээр илрүүлэх чадвартай.

# POC FOR NATIONAL ANTI-FRAUD SOLUTION MONGOLIA

# POC for National Antifraud Solution Mongolia

## Overview


**ЗОРИЛГО**

- **Шийдлийг баталгаажуулах** – **Төвлөрсөн Hub**-ээр дамжуулан **end-to-end** дуудлагын баталгаажуулалтыг **турших**
- **CLI spoofing-ээс сэргийлэх** – Үндэсний болон олон улсын хоорондын холболтын түвшинд **хуурамч дуудлагыг блоклох**
- **Нийцлийг хангах** – Үндэсний харилцаа холбооны аюулгүй байдлын зохицуулалтын шаардлагыг биелүүлэх

**ГОЛ KPI-УУД (KEY KPIs)**

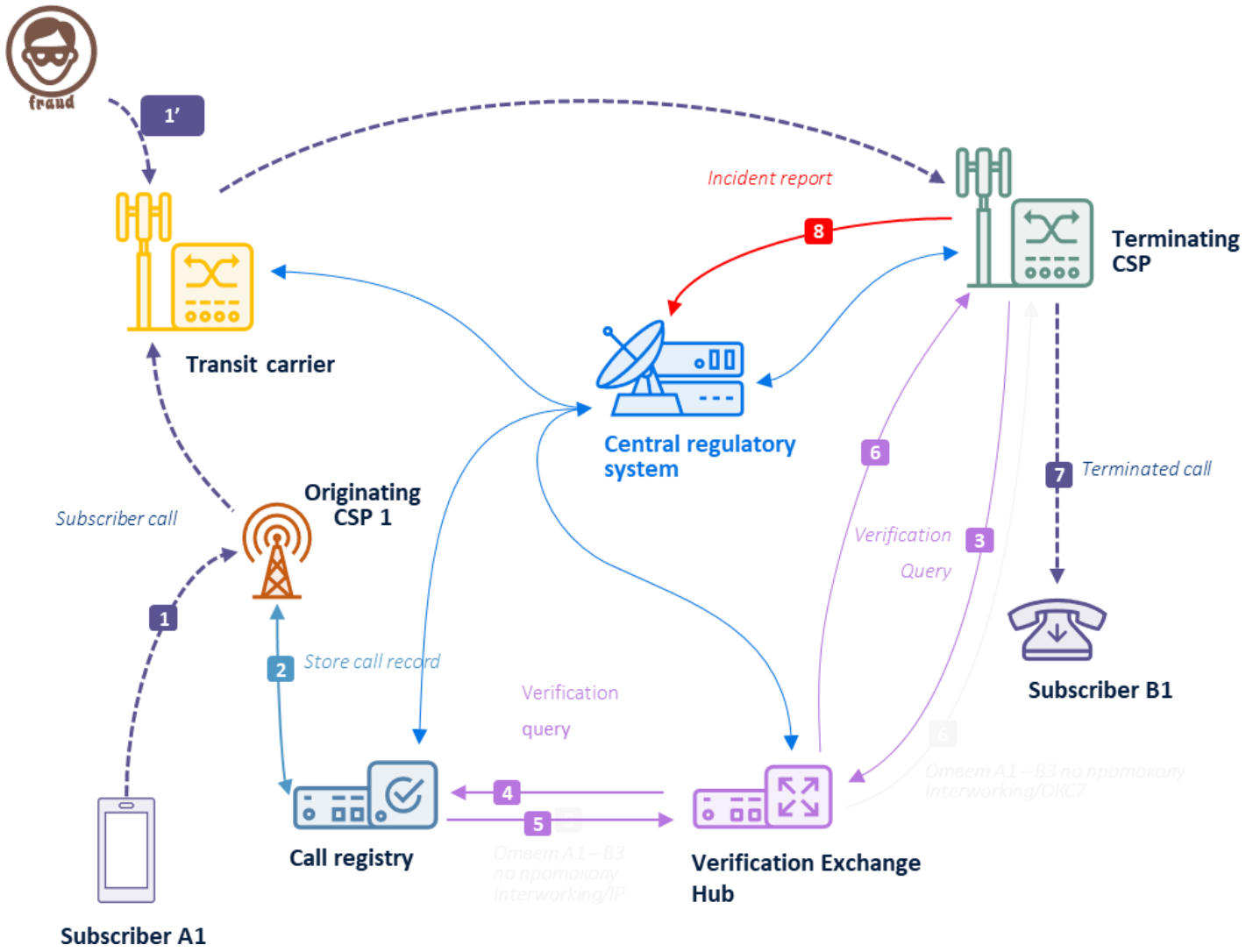
- **>99% нарийвчлалтайгаар spoofing дуудлагыг илрүүлж/блоклох**
- Туршилтад оролцож буй **хоёр операторын** дугаарлалтын төлөвлөгөөг бүрэн хамруулах
- **Real time баталгаажуулалт** – хамгийн бага хоцрогдолтой ажиллах
- **Incident and statistic тайлан** – зохицуулагч байгууллагад хүргэх

**ХЭРЭГЖИЛТ ХОЁР УЕ ШАТТАЙ:**

**1.PROOF-OF-CONCEPT (POC)** – Монгол улсын харилцаа холбооны сүлжээнд **бага хэмжээний системийг байршуулж, туршиж**, зохицуулагчийн шаардлагад нийцэж буй эсэхийг баталгаажуулах.

**2.PRODUCTION DEPLOYMENT** – POC-ийн үр дүнд үндэслэн бүрэн хэмжээнд, **том цар хүрээтэйгээр** нэвтрүүлэх.

# POC FOR NATIONAL ANTI-FRAUD SOLUTION MONGOLIA




**Хэрхэн ажилладаг вэ?**

- Үндэсний нэгдсэн системийн дотоод холболтын аль ч цэг дээр үндэсний дугаарыг spoof хийх боломжгүйг хянана.

**POC-ийн хамрах хүрээ:**

- Хоёр операторын дугаарыг бусад бүх оператор болон олон улсын операторуудтай хийсэн холболтын аль ч цэг дээр spoof хийх боломжгүйг баталгаажуулна.

**Ажиллах зарчим:**

- Дуудлагын **end-to-end баталгаажуулалт** нь **out-of-band HTTP болон SS7 протокол** дээр суурилсан **PULL MODEL**-д суурилдаг (В оператор дуудлага байгаа эсэхийг А операторооос лавлаж асуудаг).
- Дуудлага үүсгэгч оператор дуудлагыг **Local registry**-дээ бүртгэнэ.
- Дуудлага хүлээн авагч оператор дуудлага ирэх үед **registry** рүү лавлагаа илгээн тухайн дуудлага үнэхээр байгаа эсэхийг баталгаажуулна.
- Бүх лавлагаа нь **үндэсний verification backbone**-оор дамжин хийгдэнэ.

# POC FOR NATIONAL ANTI-FRAUD SOLUTION MONGOLIA

## ШИЙДЛИЙН ҮНДСЭН ҮЙЛ АЖИЛЛАГАА

**1.Ерөнхий**

•Real time дуудлага болон SMS баталгаажуулалт, CLI spoofing-ээс сэргийлэх.

•Сүлжээний үйл ажиллагаанд **маш бага саатал** (≤500ms) үүсгэх.

•PSTN (Public Switched Telephone Network) төв хэсэг түр саатсан ч үйлчилгээ (дуудлага, SMS) доголдохгүй.

**2.Бүх операторуудын хамралт**

•Бүх операторууд NAS-д нэгдэх ёстой. CSP-д зориулсан шийдлүүд багтсан.

**3.Дотоодын дуудлага**

•Дотоодын CLI-аас Монголын дугаар руу чиглэсэн 100% дуудлагыг баталгаажуулна.

•Олгогдоогүй дугаар, баталгаажаагүй хэрэглэгчийн дуудлагыг хаана.

•Гадаадаас дотоодын CLI ашигласан дуудлагыг (**роумингээс бусад**) хаана.

**4.Олон улсын дуудлага**

•Олон улсын дуудлагыг **Үндэсний Clearing House**-оор нэгдсэн байдлаар хянаж, блоклох.

•Зохицуулагчийн бүрэн хяналт дор AI/статистик суурьтай шүүлт хэрэгжүүлэх.

•Олон улсын verification системүүдтэй холбогдох өргөтгөх боломжтой архитектур.

•Гадагш чиглэсэн олон улсын дуудлагад ч мөн адил хяналт, блок хийх боломжтой.

**5.SMS баталгаажуулалт (дараагийн шат)**

•Дотоодын CLI-аас Монголын дугаар руу чиглэсэн бүх SMS-ийг баталгаажуулах.

•Олгогдоогүй дугаарын SMS, spoofed “national-like” дугаарын SMS-ийг хаах.

•Олон улсын P2P, A2P SMS-ийг олон улсын gateway дээр шүүх.

**6.Өгөгдөл хадгалалт (Retro data)**

•Дуудлагын баталгаажуулалтын EDR өгөгдлийг дор хаяж 12 сар хадгалах.

•Зохицуулагч болон эрх бүхий байгууллага API-гаар хандах боломжтой.

**7.Хяналт ба тайлагнал**

•Систем болон CSP түвшинд өргөн хүрээтэй мониторинг, тайлагнал, шалгалтын хэрэгсэлтэй.

**8.Чиглүүлэлт (Verification hubs)**

•Verification hub-уудын нөөц давхар холболт бүхий backbone-оор баталгаажуулалтын хүсэлтүүдийг дамжуулна.

•Чиглүүлэлт нь дугаарлалтын төлөвлөгөө болон MNP (Mobile Number Portability)-д суурилна.

•Verification hub-ууд нь газарзүйн хувьд давхар хамгаалалттай (geo redundancy).

**9.Эрх бүхий байгууллагад зориулсан боломжууд**

•API-гаар тодорхой шалгуур, дүрмийн дагуу ачаалал блоклох боломжтой.

**10.Банкны antifraud API (дараагийн шат)**

•Банк болон бусад зөвшөөрөгдсөн байгууллагад хэрэглэгчийн/SIM-ийн статус олгох API.

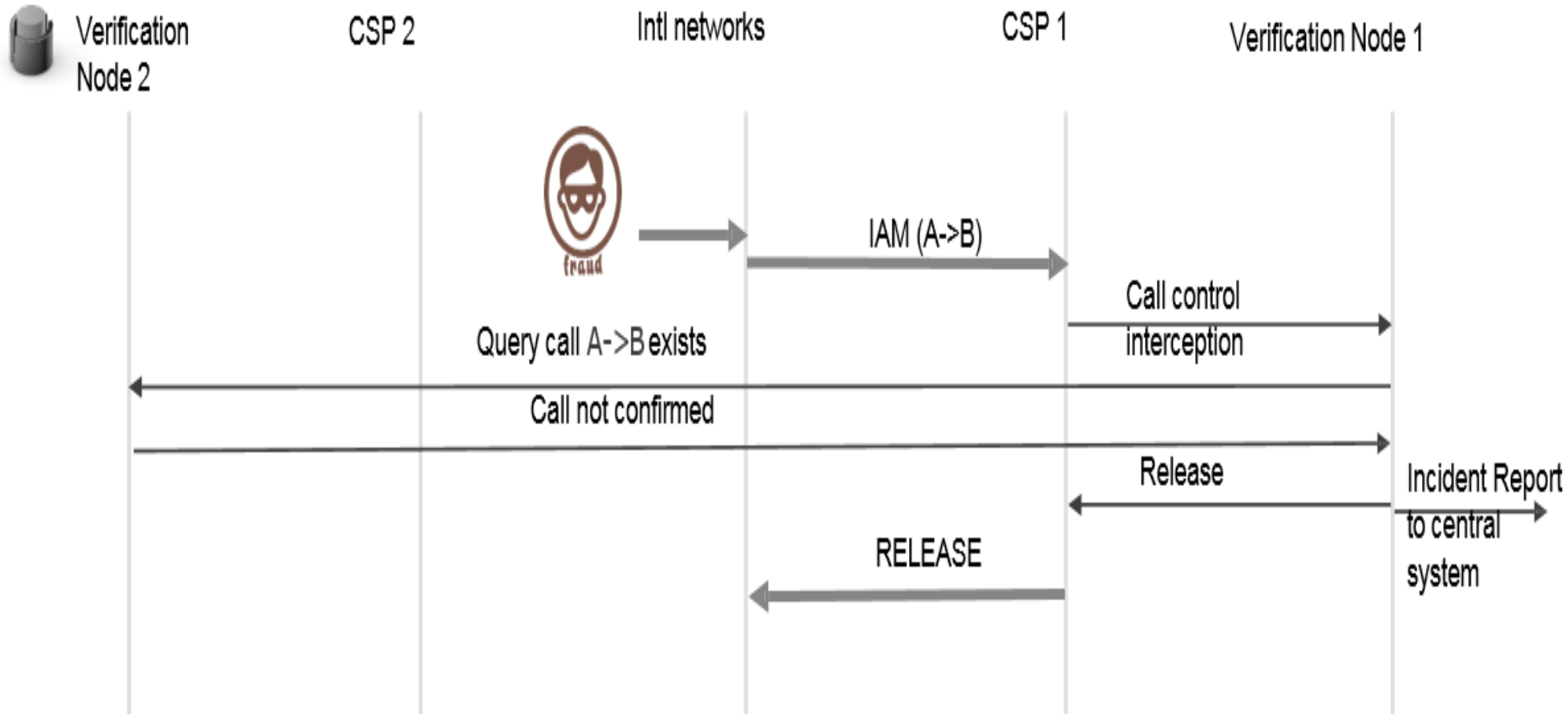
**11.Өргөтгөх боломж**

•Системийг зохицуулалтын шаардлагад нийцүүлэн өөрчлөх, өргөтгөх боломжтой.

•CSP интерфейсүүдийн ихэнхийг хамарч, интеграцийн ажлыг гэрээний дагуу гүйцэтгэнэ.

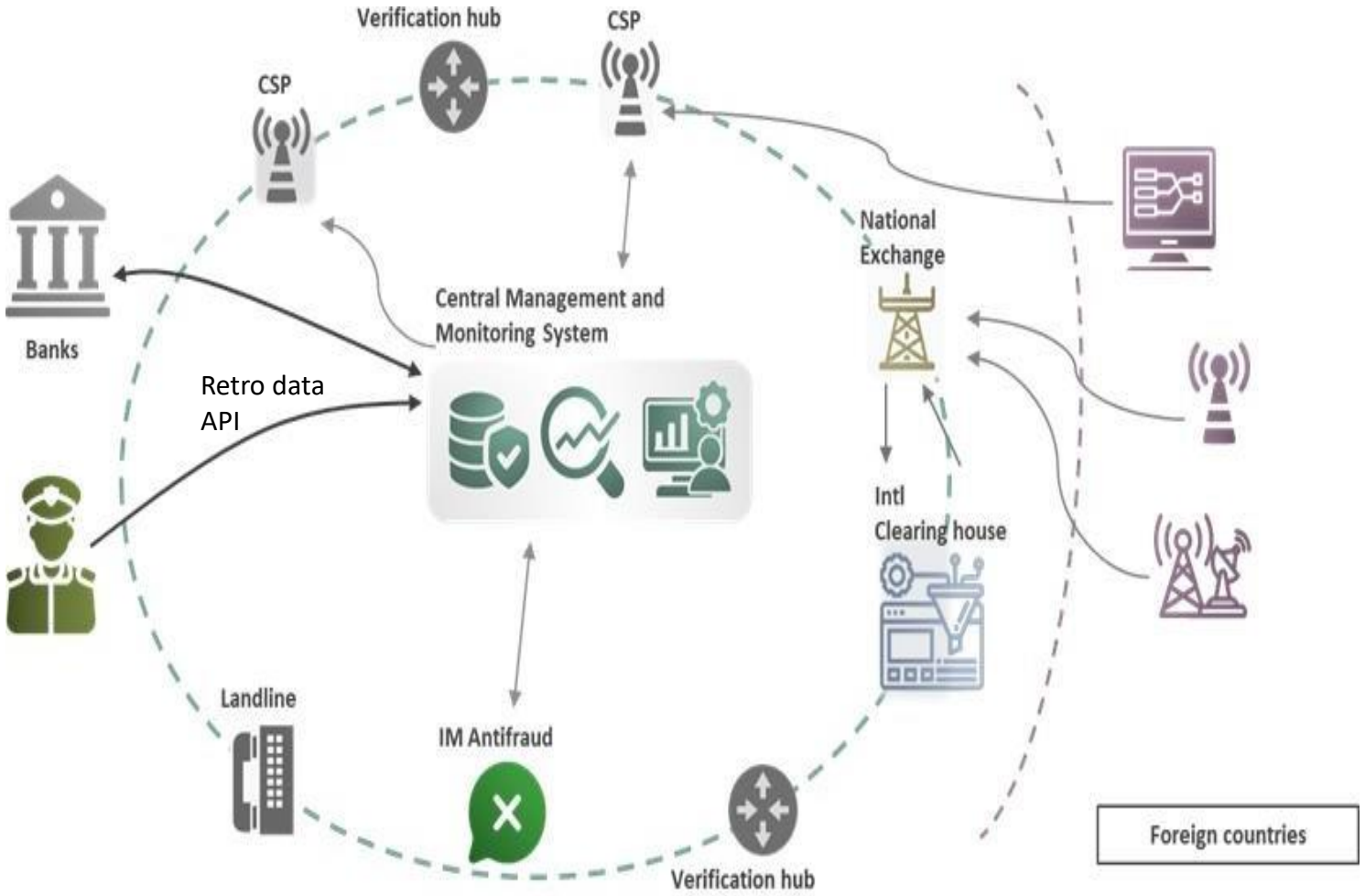
# POC FOR NATIONAL ANTI-FRAUD SOLUTION MONGOLIA

## VERIFICATION CALL FLOW (FRAUD CASE)-ДУУДЛАГА БАТАЛГААЖУУЛАЛТЫН ПРОЦЕСС



# POC FOR NATIONAL ANTI-FRAUD SOLUTION MONGOLIA

## NAS ҮНДСЭН БҮРЭЛДЭХҮҮН ХЭСГҮҮД

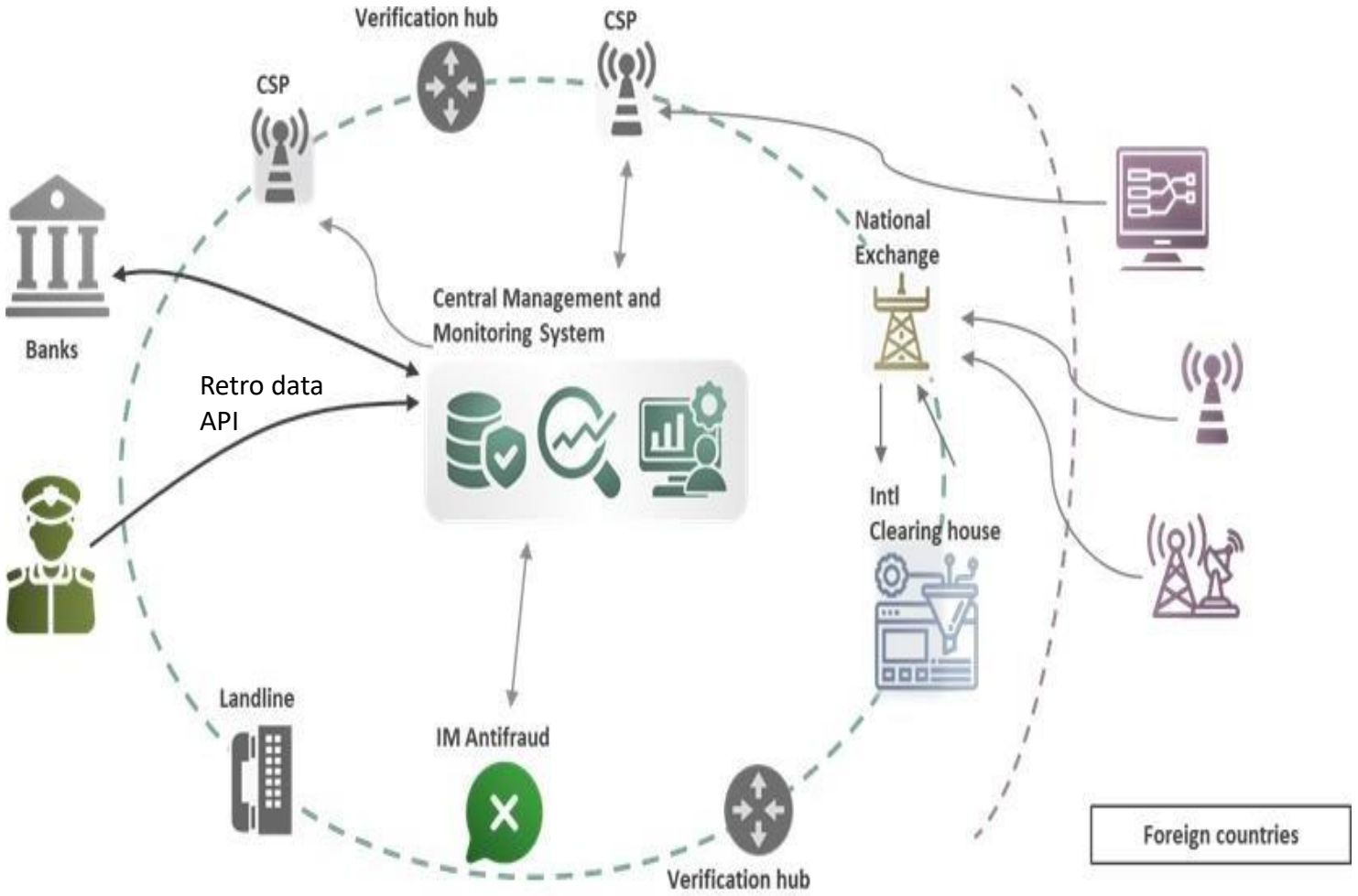



**Архитектурын шийдэл**

- **Төвлөрсөн удирдлага ба хяналтын систем** – Зохицуулагчийн удирдлага дор операторын бүртгэл, blacklist, дугаарлалт, мэдээлэл солилцоо, банк болон байгууллагуудад зориулсан нэгдсэн API.
- **Verification Exchange Hub** – Бүх операторыг холбосон backbone-оор real-time мэдээлэл дамжуулалт, чиглүүлэлт, протокол хөрвүүлэлт, traffic шүүлт, олон улсын дуудлагын цэвэрлэгээ.
- **CSP Verification Node** – CSP талд байрлаж дуудлага, SMS баталгаажуулалт хийж бүртгэл, түүх хадгалалт, лавлагаа хийнэ (жижиг CSP-д **cloud module** ашиглаж болно жишээ нь: MNO → MVNO).
- **Олон улсын траффик цэвэрлэгээний төв** – Дуудлага, мессежийг AI-аар цэвэрлэх, гадаад verification системтэй холбогдох.
- **Банкны дэд систем** – Банканд зориулсан шалгалтын API.
- **Онцгой үйлчилгээний дэд систем** – Эрх бүхий байгууллагад мөрдөн шалгах, traffic блоклох, лавлагааны API.

# POC FOR NATIONAL ANTI-FRAUD SOLUTION MONGOLIA

## NAS ҮНДСЭН БҮРЭЛДЭХҮҮН ХЭСГҮҮД- VERIFICATION EXCHANGE HUB




**Архитектурын шийдэл**

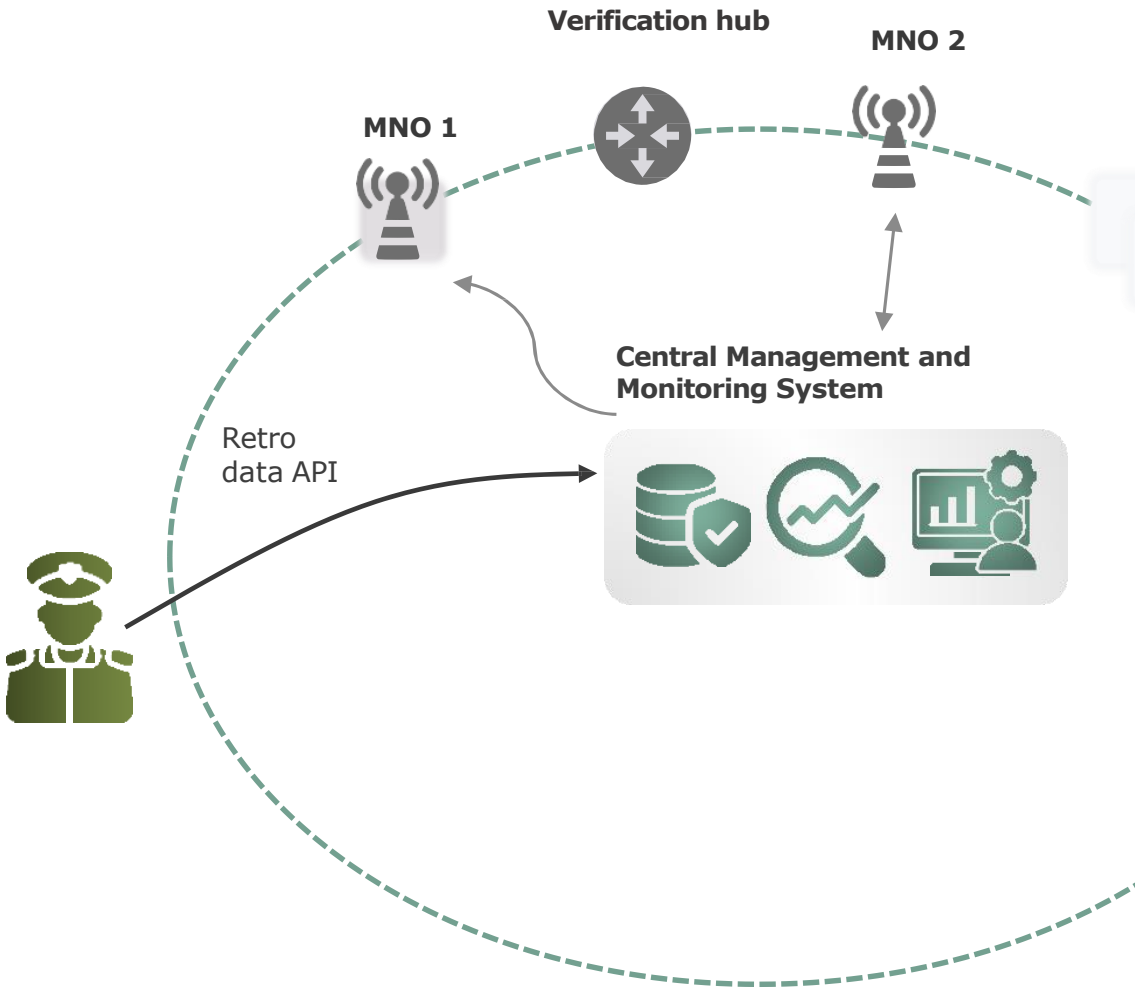
**VERIFICATION HUB** нь харилцаа холбооны операторуудын хоорондын харилцан үйлчлэлийг зохион байгуулах зориулалттай **switching ба routing node** юм.

**Үндсэн үүргүүд:**

- Харилцаа холбооны операторуудыг NAS-д холбох;
- Verification node болон бусад зангилаанаас ирсэн хэрэглэгчийн дугаарын жинхэнэ эсэхийг баталгаажуулах хүсэлтийг боловсруулах;
- Дуудлага эхлүүлэгчийн хэрэглэгчийн дугаарын баталгаажуулалтын хүсэлтийг бусад харилцаа холбооны эсвэл verification node руу чиглүүлэх;
- Доголдол гарсан үед Redundancy болон alternative routing-ээс ажиллана.
- Түр бүртгэл хадгалж, шаардлагатай бол **Төв удирдлага ба хяналтын системд** өгөх.
- Өөрийн ажиллагааны статистик, алдааг **Төв удирдлага ба хяналтын системд** өгөх.

# POC FOR NATIONAL ANTI-FRAUD SOLUTION MONGOLIA

## САНАЛ БОЛГОЖ БУЙ PROOF-OF-CONCEPT АРХИТЕКТУР




**ХАМРАХ ХҮРЭЭ (SCOPE):**

•Холболтын бүх түвшинд (олон улсын болон дотоодын) **cross-spoofing** хийх боломжгүйг **2 MNO**-ийн хувьд баталгаажуулах.

**ТӨВ СИСТЕМ (ЗОХИЦУУЛАГЧИЙН МЭДЭЛД):**

•**Нэг hub** нөөцтэй

•Үндэсний дугаарлалтын төлөвлөгөөнд тулгуурласан (хагас автомат) чиглүүлэлт

•Ашиглалтын үеийн мониторинг

•Ашиглалтын үеийн Incident болон statistics менежмент

•Туршилтын хэрэгсэл зөвхөн хязгаарлагдмал хүрээнд ашиглах боломжтой

**CSP БАТАЛГААЖУУЛАЛТЫН ЗАНГИЛААНУУД:**

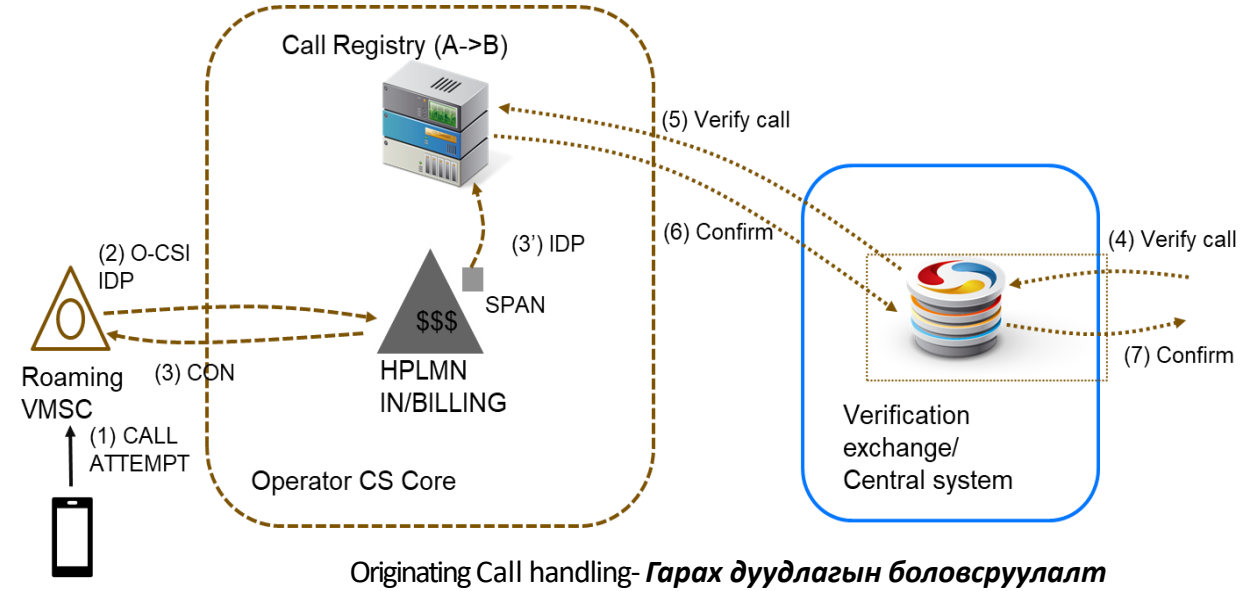
•Бүрэн ашиглалтын горимд ажиллана

•Дотоодын болон олон улсын бүх ирж буй traffic-ыг бүрэн хянах/хамрах. **Эхний шатанд зөвхөн мэдээллийн горимд ажиллана, дуудлага болон мессежийг блоклохгүй).**

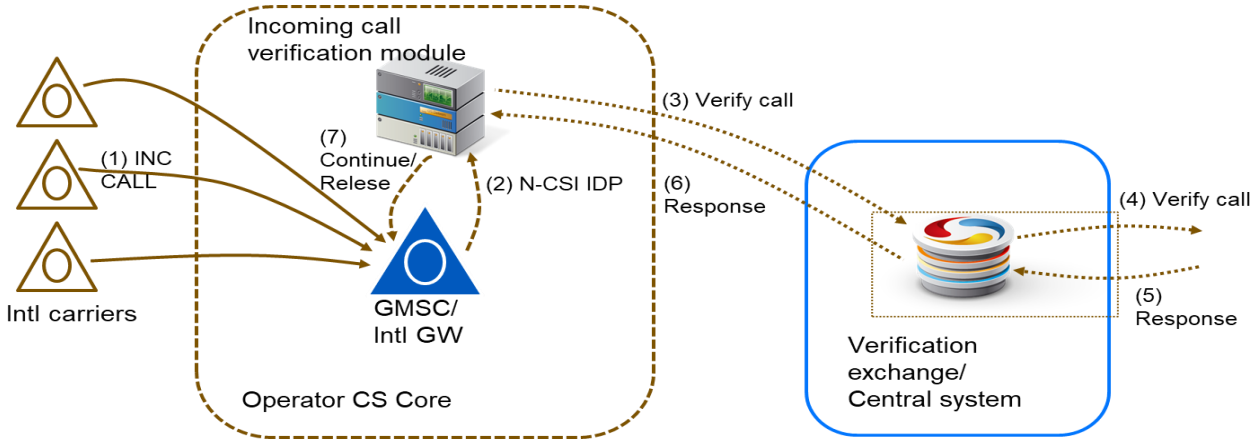
•Бүх гарах дуудлагын мэдээллийг хадгалж, баталгаажуулалтын хүсэлтийг баталгаажуулахад ашиглана

•Ашиглалтын үеийн инцидент, статистик, мэдээллийг бүрэн хадгална

# POC FOR NATIONAL ANTI-FRAUD SOLUTION MONGOLIA




Originating Call handling- ***Гарах дуудлагын боловсруулалт***




Terminating call handling ***Ирэх дуудлагын боловсруулалт***

**VERIFICATION NODE операторын сүлжээнд байрлаж,** дуудлага болон SMS-ийн баталгаажуулалтын гол үүргийг гүйцэтгэдэг үндсэн бүрэлдэхүүн юм. Энэ нь:

- Гарах дуудлага (outgoing calls) бүртгэж, verification хүсэлтийг боловсруулна
- Орох дуудлага (incoming calls) баталгаажуулна
- **Incident log** , статистик, үйл явдлын бүртгэлийг хадгална

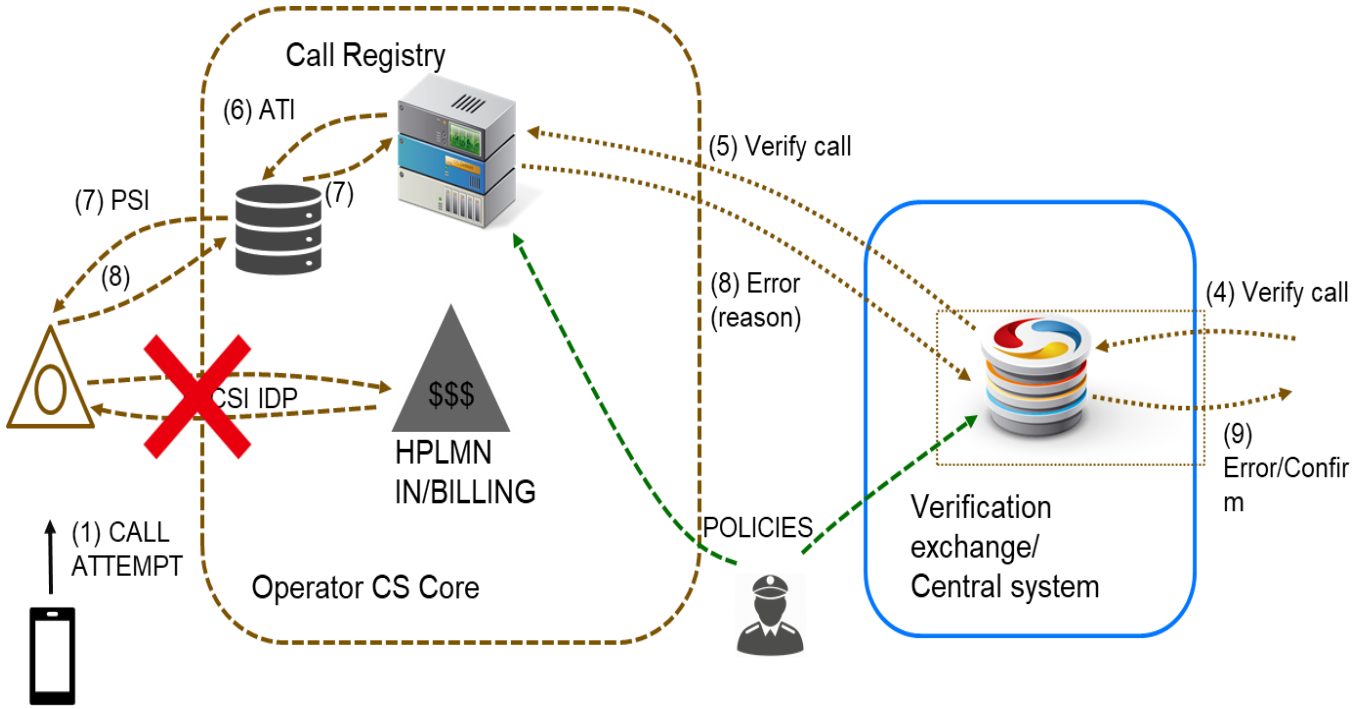
**Verification Node** ба **Verification Hubs** хоорондын **интерфейс нь:**

- **HTTP/JSON протокол дээр суурилсан** (HTTP(IP)-type Verification Node)-→ internet protocol ашиглаж verification хийх
- **CAMEL-(**Customized Applications for Mobile network Enhanced Logic) **protocol дээр суурилсан** (SS7-type Verification Node) байна. Роуминг, legacy GSM/3G сүлжээний баталгаажуулалт дээр ашиглагдана.

**Verification Node** ба **Төвлөрсөн Удирдлага, Хяналтын Систем** хооронд **SFTP протокол**-ыг ашиглана.

# POC FOR NATIONAL ANTI-FRAUD SOLUTION MONGOLIA

**Non-CAMEL роуминг дуудлагыг боловсруулах тохиолдол**




**Verification систем** нь зөвхөн ердийн дуудлага дээр ажиллахаас гадна **онцгой нөхцөлүүдэд** (corner cases) зориулсан уян хатан бодлогоор ажилладаг.

- **Яаралтай тусламжийн дуудлага (103, 102, 105 гэх мэт)** – баталгаажуулалт дээр саатахгүй, шууд нэвтрэнэ.
- **Богино код (1234, 155 гэх мэт)** – онцгой нөхцлийг таньж автоматаар зөвшөөрнө.
- **Toll-free дугаарууд (800, 1800 гэх мэт)** – тасалдахгүй байхаар тусгайлан бодлогоор зохицуулна.
- **Бусад customizable нөхцөлүүд** – төрийн болон чухал үйлчилгээний дуудлагыг whitelist хэлбэрээр хамгаална.

*CAMEL -Customized Applications for Mobile network Enhanced Logic -GSM болон 3G сүлжээнд ухаалаг сүлжээний (Intelligent Network, IN) үйлчилгээг хэрэгжүүлэх стандарчилсан платформ юм.*

# POC FOR NATIONAL ANTI-FRAUD SOLUTION MONGOLIA

## САНАЛ БОЛГОЖ БУЙ PROOF-OF-CONCEPT ИНТЕГРАЦ

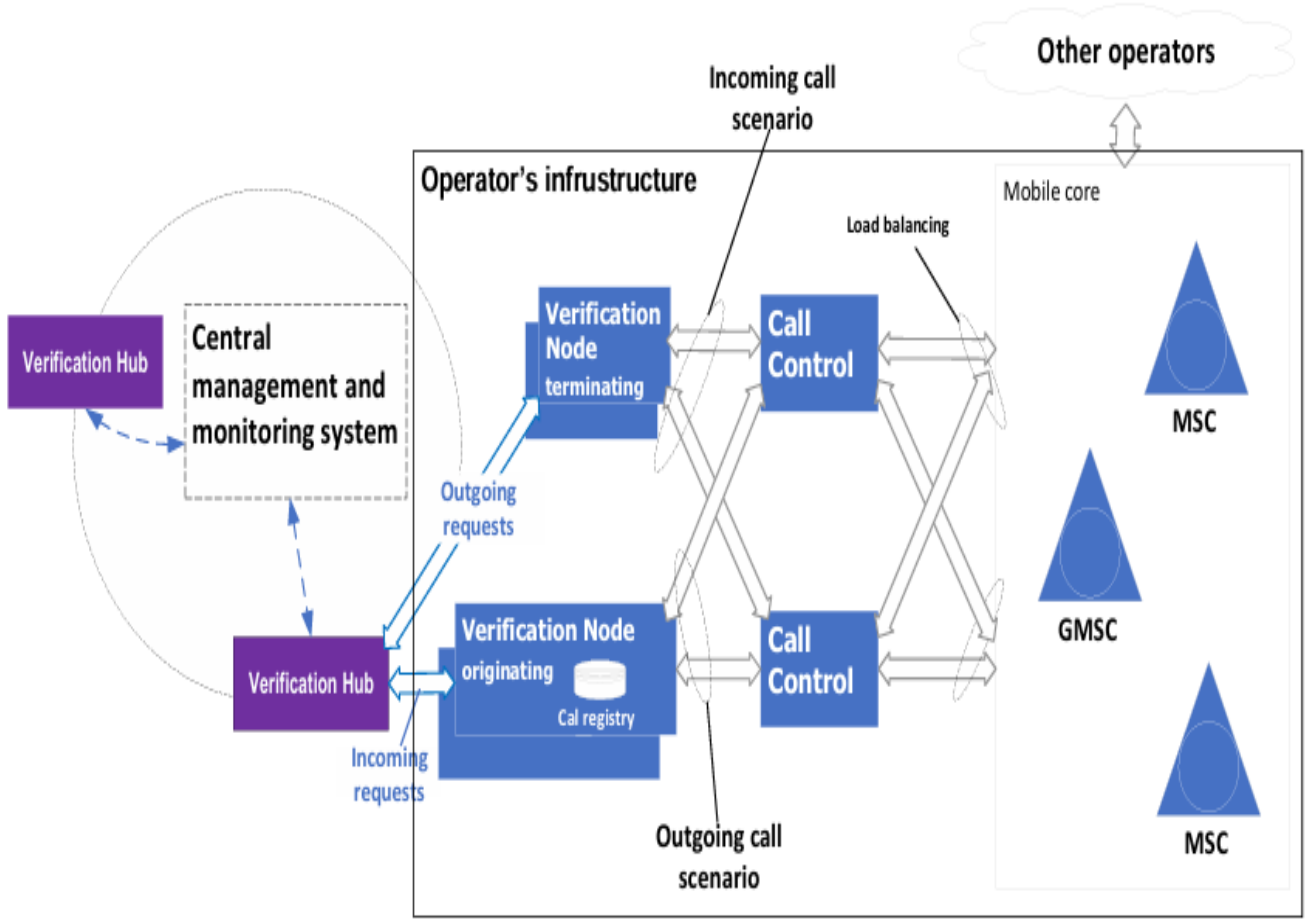



Figure 6 Integration diagram

### ХЭРЭГЖҮҮЛЭХ ҮНДСЭН ЗАРЧИМ

- **Гарах дуудлагын бүртгэл** –Гарах дуудлагын мэдээллийг бодит цагт бүртгэж, шалгана. Энэ нь **non-blocking** (дуудлагын урсгалыг тасалдуулахгүй) болон **blocking** (Verification Node түр зогсоож шалгах) горимоор хэрэгжиж болно.
- **Орж ирж буй дуудлагын баталгаажуулалт** – Бүх тохиолдолд **blocking** горимоор ажиллана. Verification Node нь дуудлагыг таслан авч шалгаад, үргэлжлүүлэх эсэх шийдвэрийг өгдөг.

### VERIFICATION NODE IDENTIFICATION & ADDRESSING

- **Identification:**
  - **Verification Node** бүрт зөвхөн нэг **давтагдашгүй ID** олгогдоно
  - ID нь **1-ээс 16,384-ийн** хооронд байна.
- **Addressing:**
  - **SS7 төрлийн Verification Node** → GT (Global Title)-ээр хаяглагддаг, spoofing-оос хамгаалагдсан байх ёстой.
  - **HTTP(IP) төрлийн Verification Node** → Verification Node ID ба тогтмол IP хаягаар тодорхойлогддог.

# POC FOR NATIONAL ANTI-FRAUD SOLUTION MONGOLIA

## САНАЛ БОЛГОЖ БУЙ PROOF-OF-CONCEPT ИНТЕГРАЦ

### OUTGOING CALL REGISTRATION

- Гарах дуудлагын мэдээллийг б**одит цагийн горимд** дуудлагын мэдээллийг **бүртгэх** ёстой (дуудлага terminating network-д хүрэхээс өмнө).
- **Бүртгэл хийх хоёр арга:**
- **Active** – дохиоллын protocol ашиглан шууд харилцах.
- **Passive** – дохиоллын мэдээллийн **mirroring** ашиглах.
- **Заавал бүртгэх мэдээлэл:**
- A-number (дуудлага эхлүүлэгч), B-number (хүлээн авагч), redirect/original дугаар, CLIP.
- Switch ID, Trunk ID, Operator ID.
- **Дугаарын мэдээлэл E.164 стандартын форматтай** байх ёстой.
- Бүртгэл нь **subscriber switch** эсвэл **transit network element**-ээс эхэлж болно.
- Операторууд **active ба passive аргыг хослуулж ашиглаж болох** ба нэг дуудлагыг хэд хэдэн удаа бүртгэх нь боловсруулалтад сөрөг нөлөө үзүүлэхгүй.

**Идэвхтэй (active):**

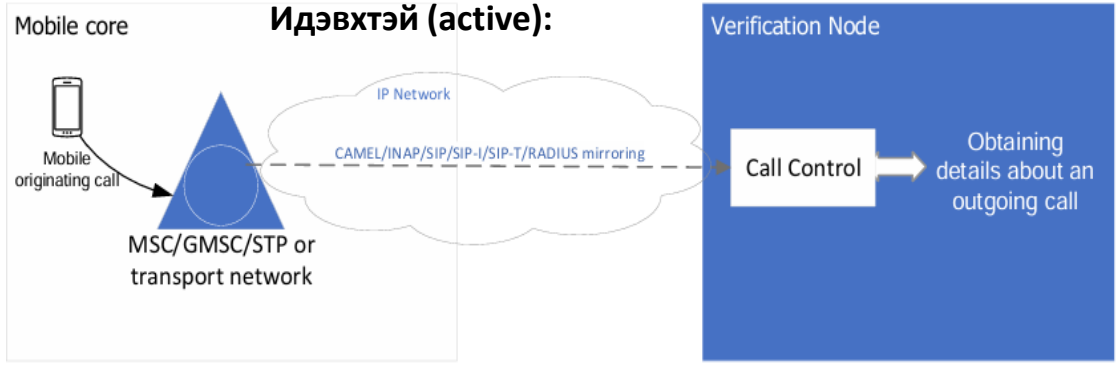



**Figure 7 Register an outgoing call. Passive monitoring.**

Supported transport protocols (IP дээр суурилсан):
•IP/SCTP/M3UA
•IP/UDP
•IP/TCP

Supported application protocols:
CAMEL/INAP
SIP / SIP-I / SIP-T

**Идэвхгүй (passive):**

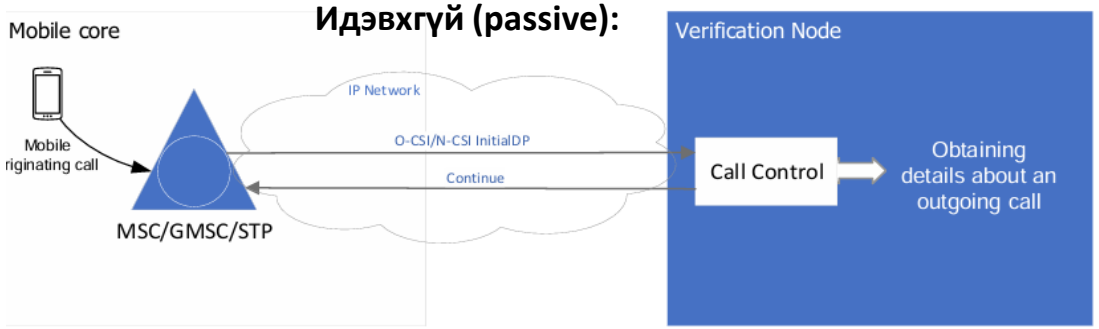



**Figure 8 Active communication with mobile core. CAMEL protocol.**

Supported transport protocols (IP дээр суурилсан):
- IP/SCTP/M3UA
- IP/UDP
- IP/TCP

Supported application protocols:
- CAMEL/INAP
- SIP / SIP-I / SIP-T

# POC FOR NATIONAL ANTI-FRAUD SOLUTION MONGOLIA

## САНАЛ БОЛГОЖ БУЙ PROOF-OF-CONCEPT ИНТЕГРАЦ

### INCOMING CALL VERIFICATION

•Орж ирэх дуудлагыг заавал **blocking mode**-оор баталгаажуулна: Verification Node дуудлагыг тасалж шалгаад үргэлжлүүлэх эсвэл цуцлах шийдвэр гаргана.

•**Операторын төхөөрөмж** нь бодит цагийн горимд дараах **мэдээллийг илгээх** ёстой: **A-number, B-number, redirect/original дугаар, CLIP, Switch ID, Trunk ID, Operator ID**.

•Дугаарын мэдээлэл **E.164 стандартын форматтай** байх шаардлагатай.

•Баталгаажуулалтыг **terminating switch node** эсвэл **transit switch** дээр хийж болно.

•Операторууд intra-switch (дотоод холболтын) дуудлага болон өөрийн хэрэглэгчдийн урсгалыг Verification Node руу заавал илгээх шаардлагагүй.

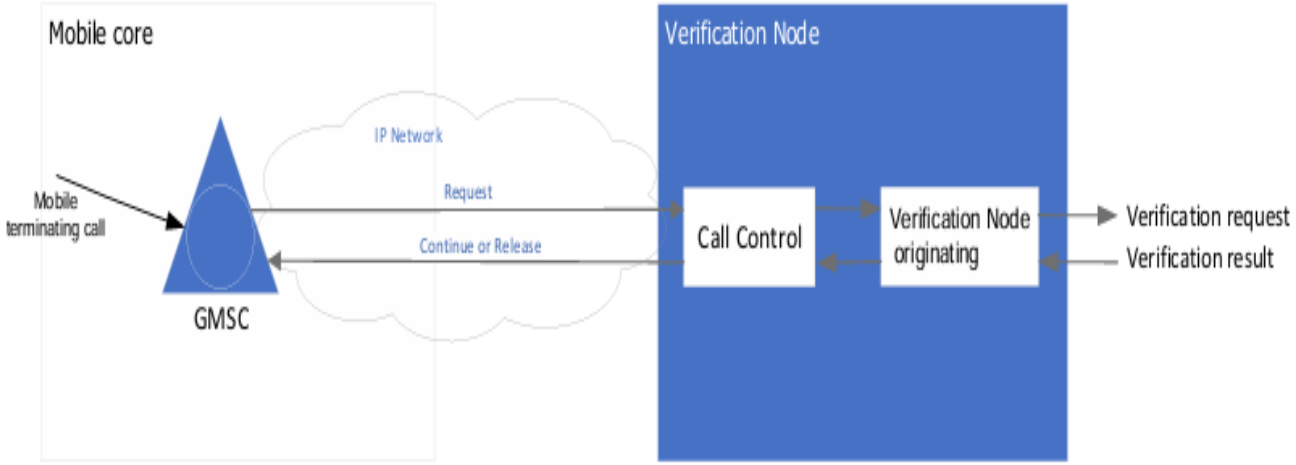



Figure 10 Incoming call verification.

•**CAMEL/INAP** болон **SIP/SIP-I/SIP-T** протоколуудыг дэмждэг.

•GMSC → Verification Node → NAS → эх оператор гэсэн урсгалаар дуудлага баталгаажуулалт явагдана.

•Амжилттай бол дуудлага үргэлжилнэ, амжилтгүй бол дуудлага таслагдана.

•Протоколын дэмжлэгийг ирээдүйд өргөжүүлэх боломжтой.

## САНАЛ БОЛГОЖ БУЙ PROOF-OF-CONCEPT REDUNDANCY

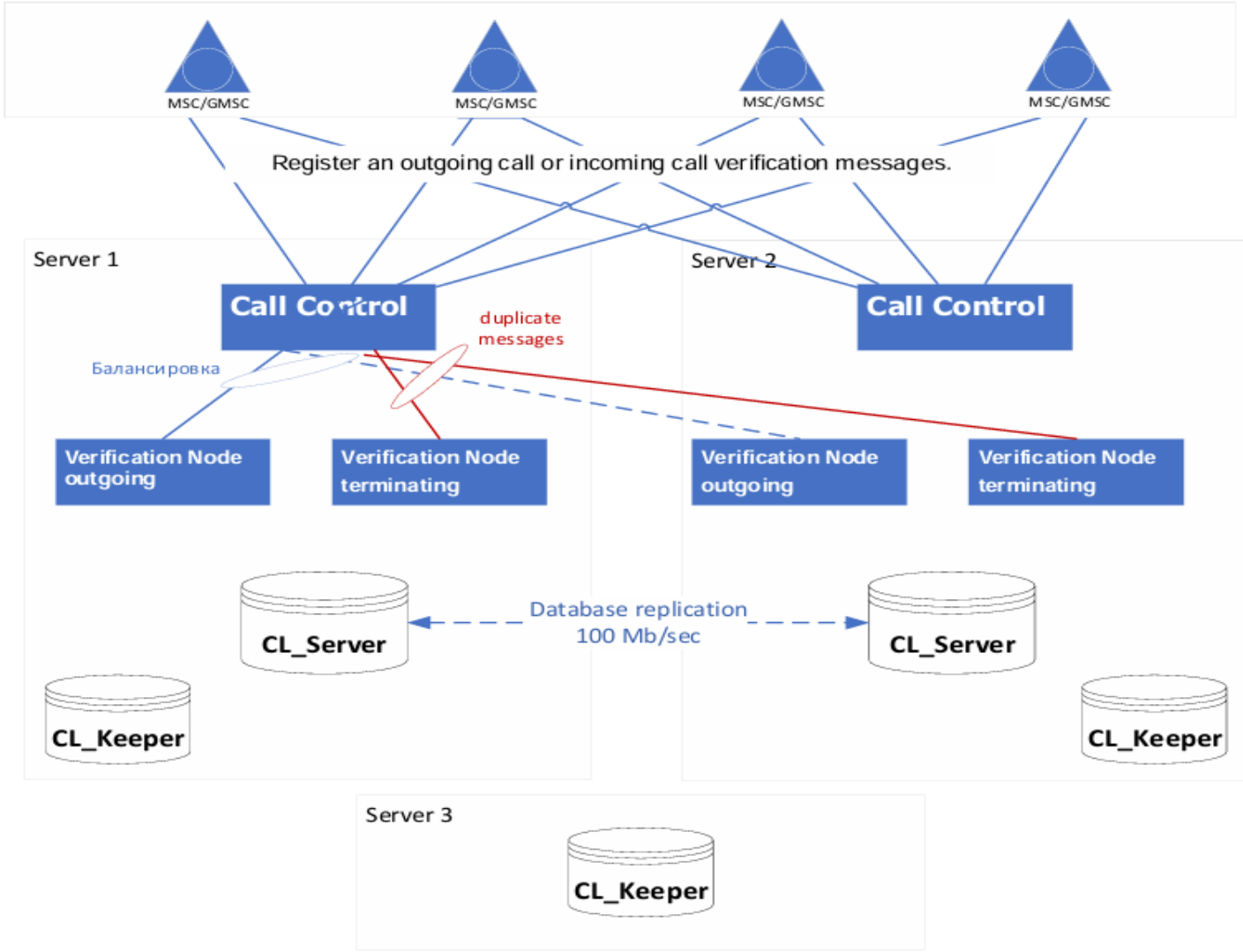



Figure 11 The redundancy diagram

- **Verification Node** нь **active-active (A-A) redundancy**-г дэмждэг бөгөөд операторын switch нь **A-A** эсвэл **active-standby (A-S)** горимоор ажиллаж болно.
- Дуудлага дамжуулах бүх модулиуд **давхар (duplicated) байх шаардлагатай.**
- MSC/GMSC-ээс ирсэн дуудлагын мэдээлэл **Call Control** Access Point-уудын хооронд **ачаалал тэнцвэржүүлэлтээр** хуваарилагдана.
- Гарах дуудлагын мэдээлэл **хоёр сервер дээр зэрэг хадгалагдаж**, орж ирэх дуудлагын мэдээлэл Verification Node-уудын хооронд **load balancing-оор** хуваарилагдана.
- **Нэг Access Point доголдвол** MSC/GMSC автоматаар нөөц Access Point руу **дахин илгээнэ.**
- Өгөгдлийн сан **гурван серверийн кластер дээр real-time replication** хийж, мэдээллийн нэгдмэл байдлыг хадгалдаг.
- Primary сервер унавал өгөгдөл **автоматаар backup сервер рүү шилжиж**, сэргээх оролдлого **60 секунд тутамд** хийгдэнэ.

# POC FOR NATIONAL ANTI-FRAUD SOLUTION MONGOLIA

## САНАЛ БОЛГОЖ БУЙ PROOF-OF-CONCEPT -HARDWARE REQUIREMENTS

POC-ийг туршилтаар харуулах зорилгоор дараах серверүүд шаардлагатай байна.

**Hardware requirements**

NAS-ийн серверийн тоног төхөөрөмж нь дараах ерөнхий шаардлагыг хангах ёстой:

- Суурилуулсан алсын удирдлагын хэрэгслүүдийг дэмжих
- **Hot-swappabl**e хатуу дискүүдийг дэмжих
- CPU SSE4.2 зааврыг дэмжих
- Backup fans болон hot-swappable цахилгаан хангамжийг дэмжих
- Dedicated service processor болон bus-д суурилсан нэгдсэн дэвшилтэт алдаа илрүүлэх системийг дэмжих
- Remote console (IPMI - серверийг алсаас удирдах **олон улсын стандарт протокол**) дэмжих

Системийг **физик сервер** эсвэл **виртуал машин** дээр ажиллуулах боломжтой.

**Verification module** нь операторын байрлалд байрлана. Нарийвчилсан техникийн үзүүлэлтүүдийг оператортой зөвлөлдсөний дараа гаргаж өгнө. Redundant тохиргоонд 3 сервер шаардлагатай, харин хамгийн бага тохиргоонд нэг сервер байхад хангалттай. Ийм тохиргоо MNO бүрт шаардагдана.

**CENTRAL MANAGEMENT AND MONITORING SYSTEM**

| Server | Quantity | CPU cores | RAM | Disk capacity | Networking | Operation system |
|---|---|---|---|---|---|---|
| Frontend/Backend servers/Monitoring | 1 | processor 3 GHz or higher with SSE4.2 support 16 cores | 64 G | SSD, 1TB, redundancy | 1000Base-T | Debian 11 and higher |

**VERIFICATION HUB**

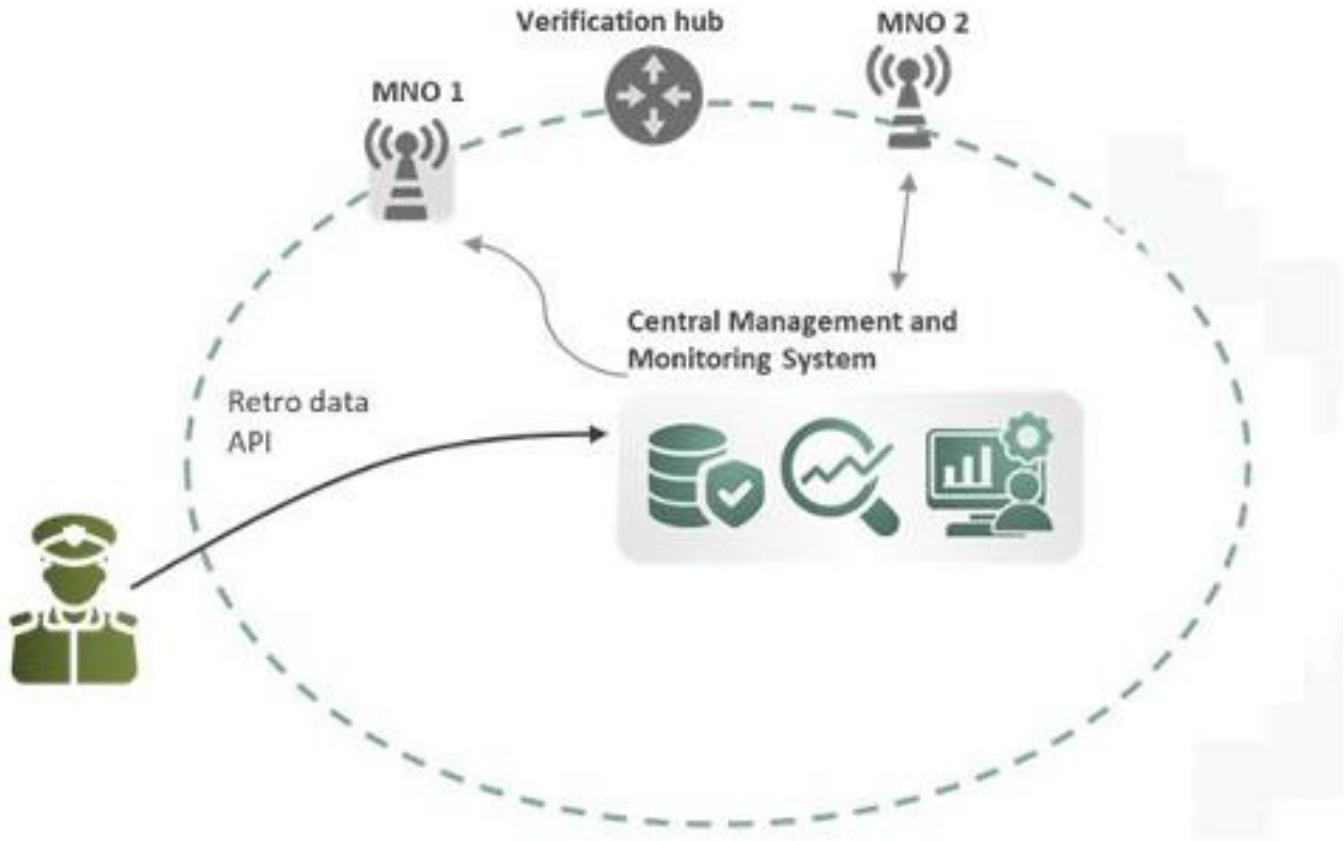
| Server | Quantity | CPU cores | RAM | Disk capacity | Networking | Operation system |
|---|---|---|---|---|---|---|
| Processing server | 2* | processor 3 GHz or higher with SSE4.2 support 16 cores | 64 GB | SSD, 500G, redundancy | 1000Base-T | Debian 11 and higher |

**VERIFICATION MODULE**

| Server | Quantity | CPU cores | RAM | Disk capacity | Networking | Operation system |
|---|---|---|---|---|---|---|
| Processing server | 3* | processor 3 GHz or higher with SSE4.2 support 16 cores | 32 GB | SSD, 500G | 1000Base-T | Debian 11 and higher |

# POC FOR NATIONAL ANTI-FRAUD SOLUTION MONGOLIA

## САНАЛ БОЛГОЖ БУЙ PROOF-OF-CONCEPT REMOTE ACCESS




**Алсын хандалт (Remote access)**

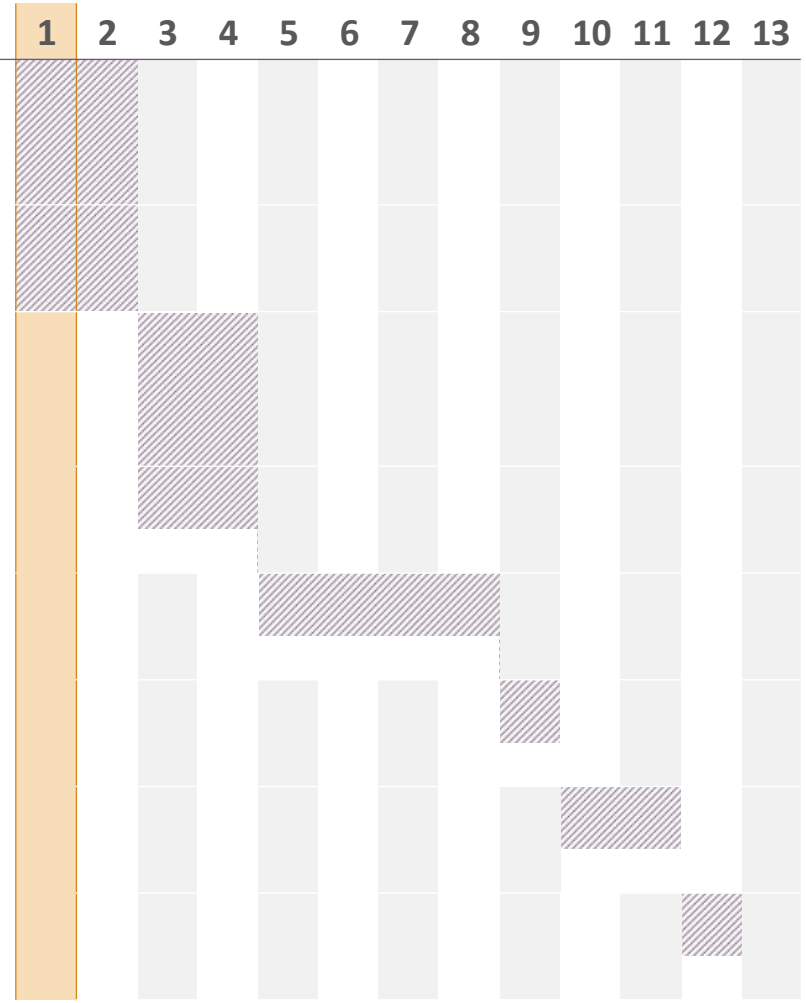
Бүх серверүүдэд шийдлийг **нэвтрүүлэх, хянах, дэмжлэг үзүүлэх** зорилгоор алсын хандалт хийх боломжтой байх ёстой.
Дор хаяж дараах портууд нээлттэй, хандалт хийх боломжтой байх шаардлагатай:

- **23 (SSH)**
- **443 (HTTPS)**
- **80 (HTTP)**

Хандалтыг заавал **аюулгүй сувгаар** (жишээ нь: VPN, зөвхөн зориулагдсан IP-ээс нэвтрэх, эсвэл түүнтэй төстэй технологи) хийх ёстой.

# Execution plan

| ACTIVITY | RESPONSIBLE | PLAN START (WEEK #) | PLAN DURATION (WEEKS) |
|---|---|---|---|
| Hardware and channels preparation (CRC) | CRC | 1 | 2 |
| Hardware and channels preparation (2 operators) | Operators | 1 | 2 |
| Central system and hubs rollout and base configuration | Hex Labs | 3 | 2 |
| Operators systems base deployment | Hex Labs | 3 | 2 |
| Operators core network integration | Operators/Hex labs | 5 | 4 |
| System tests | Operators/Hex labs/CRC | 9 | 1 |
| System test zone | Operators/Hex labs/CRC | 10 | 2 |
| POC Evaluation | CRC/Hex Labs | 12 | 1 |



# IM Deactivation Solution Requirements for POC, Mongolia

## Overview


**ЗОРИЛГО:**

**IM Deactivation (**Instant Messaging Deactivation) шийдэл нь үндэсний зохицуулалтын шаардлагыг зөрчсөн эсвэл залилангийн үйл ажиллагаатай холбогдсон **WhatsApp болон Telegram аккаунтыг автоматаар устгах** ажиллагааг хэрэгжүүлнэ.

**ШИЙДЛИЙН ҮЙЛ АЖИЛЛАГАА**

Шийдлийн гол функцууд нь дараах байдлаар:

- Хэрэглэгчийн дугаарууддтай (MSISDN) холбогдсон WhatsApp/Telegram **аккаунтыг автоматаар илрүүлэх.**
- Урьдчилан тодорхойлсон жагсаалтад багтсан MSISDN-үүдийн аккаунтыг бүрэн **автоматаар устгах**.
- Операторууд болон зохицуулагчдад зориулсан иж бүрэн **тайлан**.

# IM DEACTIVATION SOLUTION REQUIREMENTS FOR POC, MONGOLIA

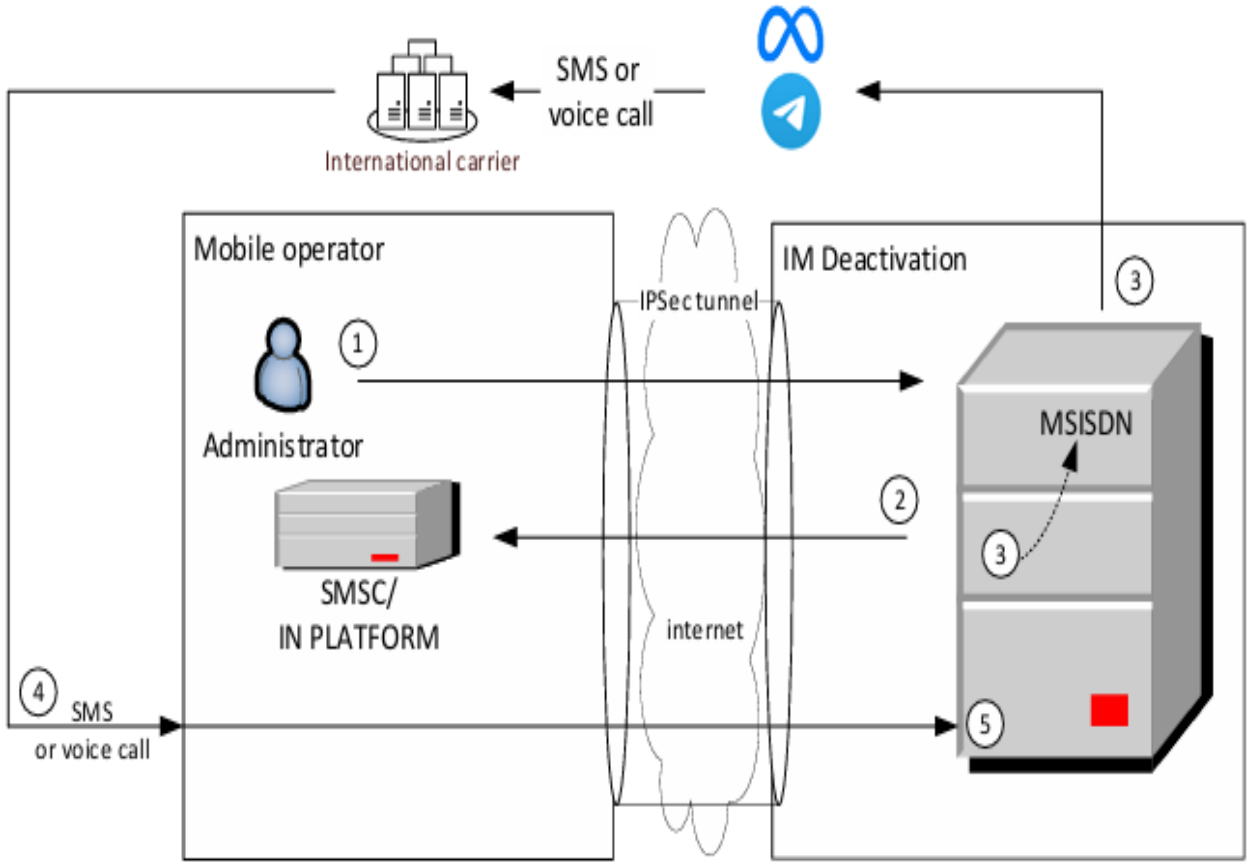



Figure 1 Basic principle of operation

**IM Deactivation шийдлийн үндсэн үйл явц:**

- Оператор **MSISDN** (Mobile Station International Subscriber Directory Number-**E.164 стандарт** дээр суурилагдсан олон улсын форматтай гар утасны хэрэглэгчийн бүрэн дугаар) жагсаалтыг **системд байршуулна** (WEB/API эсвэл SFTP-ээр).
- Хэрэгцээтэй тохиолдолд MSISDN-ийг SMSC/IN **платформд дамжуулж** болно.
- Систем жагсаалтад багтсан MSISDN-үүдийг **устгах процессыг эхлүүлнэ**.
- WhatsApp/Telegram-аас ирсэн **OTP** (SMS/дуудлага)-г оператор **хүлээн а**вна.
- IM Deactivation нь OTP-г ашиглан тухайн **аккаунтыг автоматаар идэвхгүйжүүлнэ**.

# IM DEACTIVATION SOLUTION REQUIREMENTS FOR POC, MONGOLIA

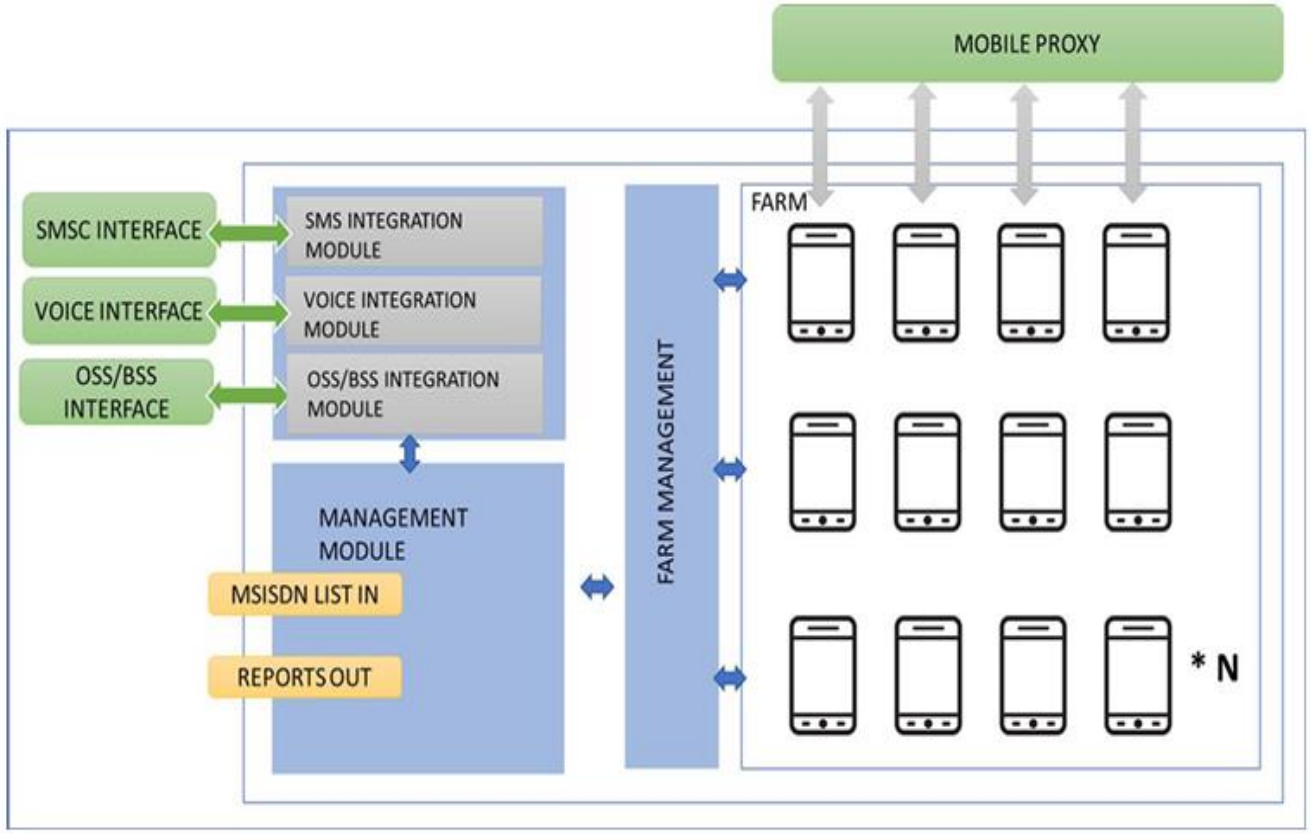



**Figure 2 General solution architecture**

**Ерөнхий архитектур**

**1.Management Module** – удирдлага, автоматжуулалт, дансны аудит, устгал, өгөгдөл хүлээн авах, тайлан гаргах.

**2.SMS Integration Module** – OTP мессеж хүлээн авах, MSISDN жагсаалт удирдах, операторын SMS төв болон бизнесийн системтэй API-р холбогдож мэдээлэл солилцоно.

**3.Voice Integration Module** – OTP дуудлага хүлээн авах, CAMEL/SIP интерфэйс, IVR/Speech Recognition.

**4.OSS/BSS Integration Module** – хэрэглэгчийн төлөв шалгах (идэвхгүй эсэх).

**5.Managed Android Farm** – эмулятор/жижиг төхөөрөмжөөр WhatsApp/Telegram руу хандалт хийх.

•**Database** – дугаарын мэдээлэл, устгалын оролдлогын бүртгэл болон бусад дотоод мэдээллийг хадгална

**1.Distributed Proxy Infrastructure** –аюулгүй байдал болон ачаалал хуваарилахад ашиглагдана.

# IM DEACTIVATION SOLUTION REQUIREMENTS FOR POC, MONGOLIA

## САНАЛ БОЛГОЖ БУЙ PROOF-OF-CONCEPT ARCHITECTURE

**ШИЙДЭЛД ТАВИГДАХ ИНТЕГРАЦИЙН ШААРДЛАГА**

Энэхүү шийдэл нь мобайл **операторын дэд бүтцэд интеграц хийх**ийг шаарддаг. Meta эсвэл Telegram-аас нэг удаагийн нууц үг (OTP) авахын тулд хоёр төрлийн интеграц хэрэгтэй:

- **SMS integration**
- **Voice integration**

Шийдэл нь мобайл оператор болон IM deactivation системийн хоорондын холбоог хамгаалахын тулд **VPN tunnel** ашиглана. VPN-ийн тохиргоо интеграцийн үе шатанд хэлэлцэгдэнэ.

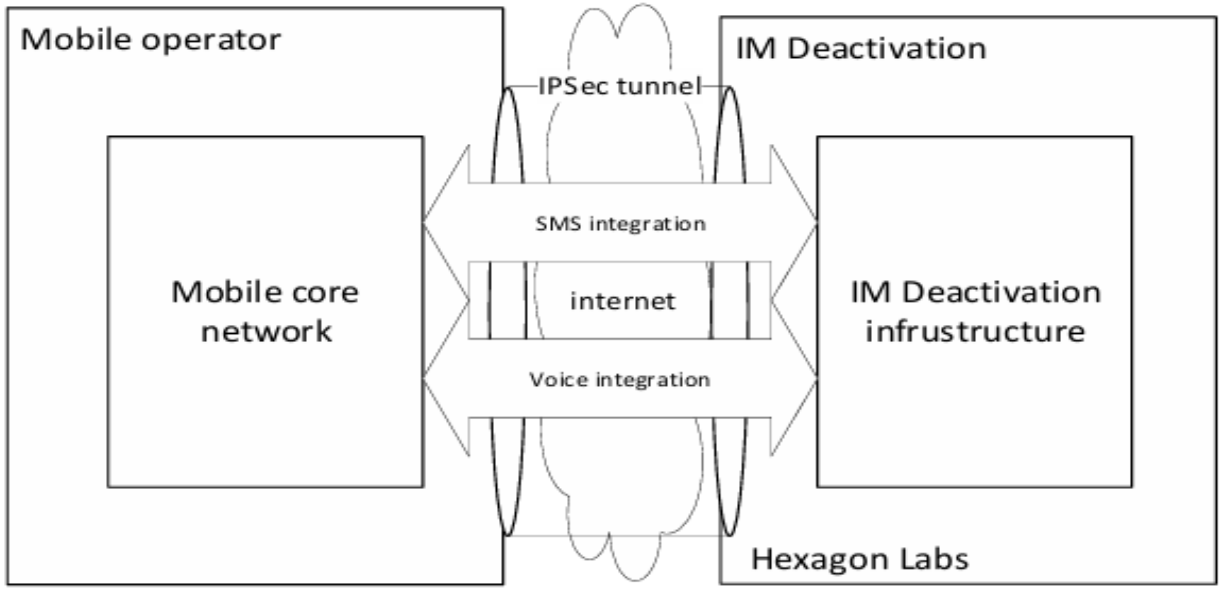



**Figure 3 Simplified POC architecture**

**УРЬДЧИЛСАН НӨХЦӨЛҮҮД (PRECONDITIONS)**

- POC-ийн хүрээнд **IM Deactivation шийдэл нь Hexagon Labs-ийн дэд бүтцэд байрлана.**
- **Мобайл оператор** болон **Hexagon Labs**-ийн дэд бүтцийн хооронд **аюулгүй холболт** тогтоох шаардлагатай.
- **Мобайл оператор** POC техникийн шийдлийг албан ёсоор **зөвшөөрнө.**
- Мобайл оператор IM deactivation шийдэлтэй **SMS болон Voice интеграц** хангана.
- **Мобайл оператор** сар бүрийн хэрэглээтэй, идэвхтэй роуминг үйлчилгээтэй **10 SIM карт**, гадаадад **5GB дата багцтай** нийлүүлнэ.
- Мобайл оператор IM устгалд ашиглах **MSISDN дугаарууд/диапазон**-ыг өгнө.
- Мобайл оператор туршилтын үйл ажиллагаанд **шууд оролцоно**.

# IM DEACTIVATION SOLUTION REQUIREMENTS FOR POC, MONGOLIA

## САНАЛ БОЛГОЖ БУЙ PROOF-OF-CONCEPT SMS INTEGRATION

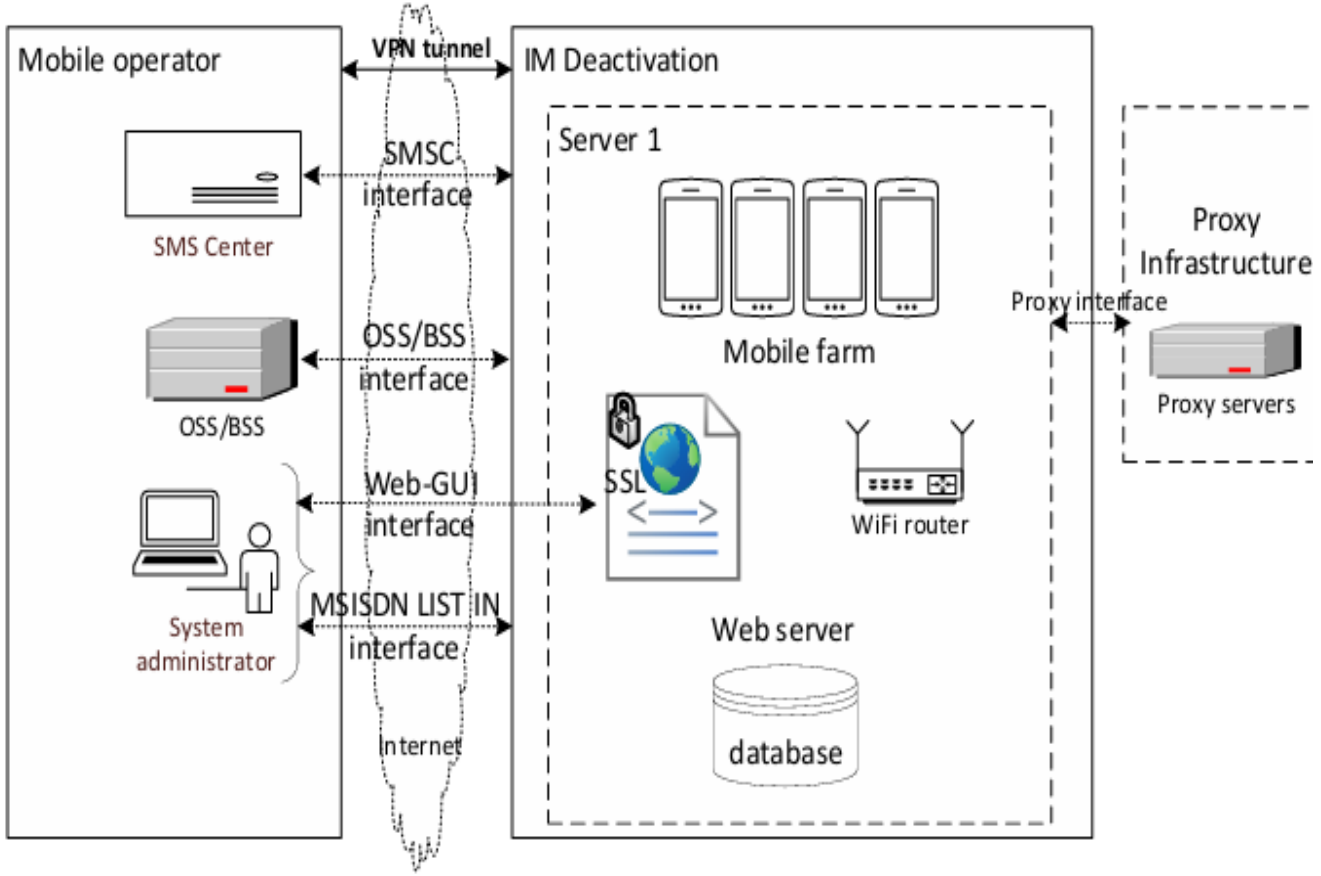



**Figure 5 SMS integration diagram**

- **SMSC interfaces**: SMPP v3.4, HTTP API (SMS whitelist болон SMS хүлээн авах), эсвэл Custom API.
- **MSISDN whitelist удирдах API** шаардлагатай бөгөөд нэг дугаарт суурилсан үйлдлийг дэмжих боломжтой байх ёстой.
- Оператор whitelist-д бүртгэгдсэн OTP SMS-ийг автоматаар дамжуулах ёстой; шаардлагатай бол **SenderID-аар SMS шүүх** боломжтой.
- Хэрэв MSISDN нь HLR дээрээс устгагдсан эсвэл блоклогдсон бол OTP SMS-ийг заавал систем рүү (шийдэл рүү) чиглүүлэх ёстой. (SMS firewall/home routing ашиглан).
- Операторын SMSC OTP SMS-ийг дор хаяж **2 минут хадгалж**, сервер холбогдмогц хадгалсан мессежүүдийг дамжуулах шаардлагатай.
- SMS-ийг **ирсэн дарааллаар нь** дамжуулж, мессеж бүр дор хаяж SenderID, B-number, Text мэдээллийг агуулсан байх ёстой.
- **Base scenario**:
  - MSISDN жагсаалтыг SMSC эсвэл SMS Firewall руу байршуулна.
  - IM Deactivation систем OTP үүсгэнэ.
  - OTP SMS сүлжээнд ирээд, SMSC-ээс шийдэл рүү дамжуулагдана.
  - Систем SMS-ийг боловсруулж, дараа нь MSISDN жагсаалтыг шинэчилнэ.

# IM DEACTIVATION SOLUTION REQUIREMENTS FOR POC, MONGOLIA

## САНАЛ БОЛГОЖ БУЙ PROOF-OF-CONCEPT VOICE INTEGRATION

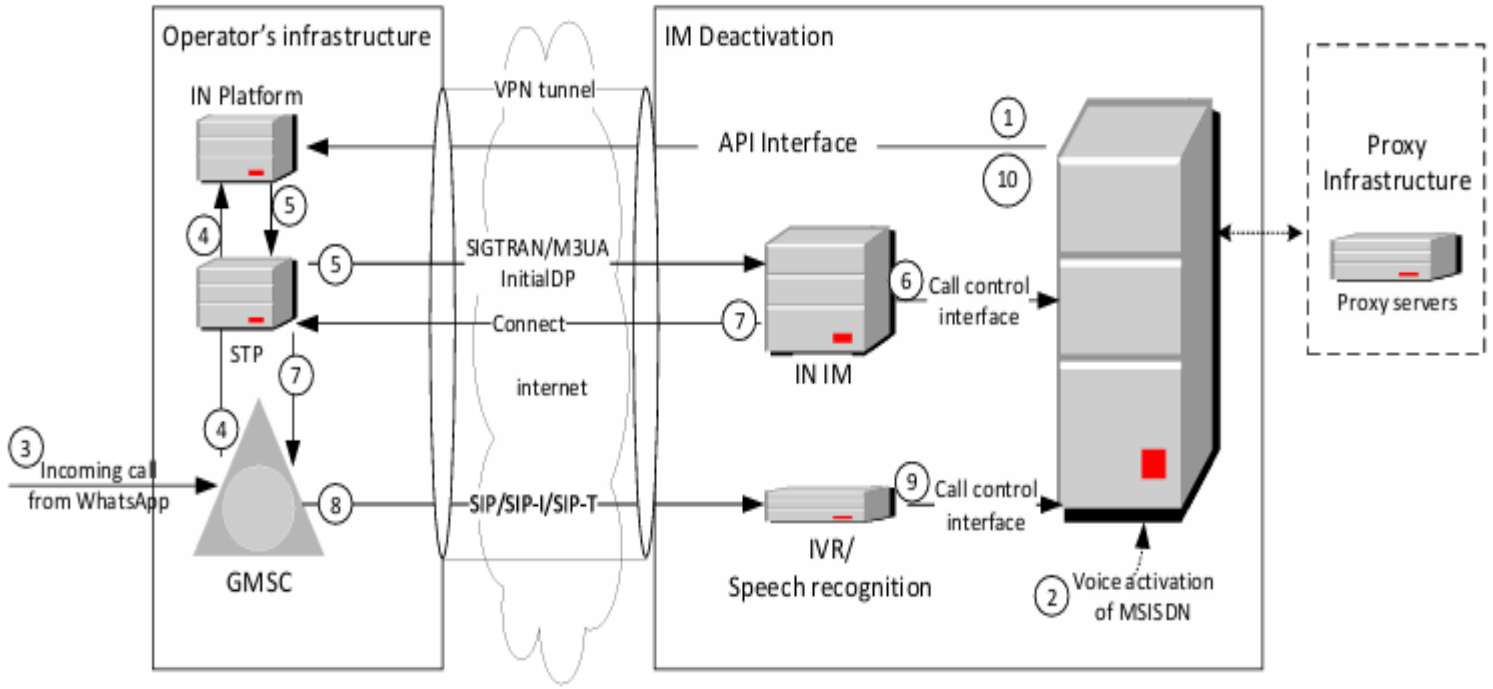



**Figure 6 Voice integration diagram**

A2P SMS ихэвчлэн блоклогдох тул OTP-г **voice call/flashcall** ашиглан авна.

- **Үндсэн интерфэйсүүд:** SCTP (IN), SIP/SIP-I/SIP-T, Call control, IN API.
- Оператор IN API-д хандалт өгөх, SIGTRAN/M3UA болон SCCP routing тохируулах, SIP trunk ба prefix маршрутыг IVR рүү чиглүүлэх.
- **Base scenario:**
- Устгах MSISDN сонгогдож, IN платформ дээр CAMEL redirect хийгдэнэ → WhatsApp/Telegram-аас ирсэн дуудлага GMSC дээр бууна → IVR рүү чиглүүлэгдэж OTP илрүүлэгдэнэ.
- **IVR-ийн үүрэг:** Дуудлагын замаас **A-number шинжилгээ** эсвэл **voice recognition** ашиглан OTP-г илрүүлж IM Deactivation систем рүү дамжуулна.

# IM DEACTIVATION SOLUTION REQUIREMENTS FOR POC, MONGOLIA

## САНАЛ БОЛГОЖ БУЙ PROOF-OF-CONCEPT VOICE INTEGRATION

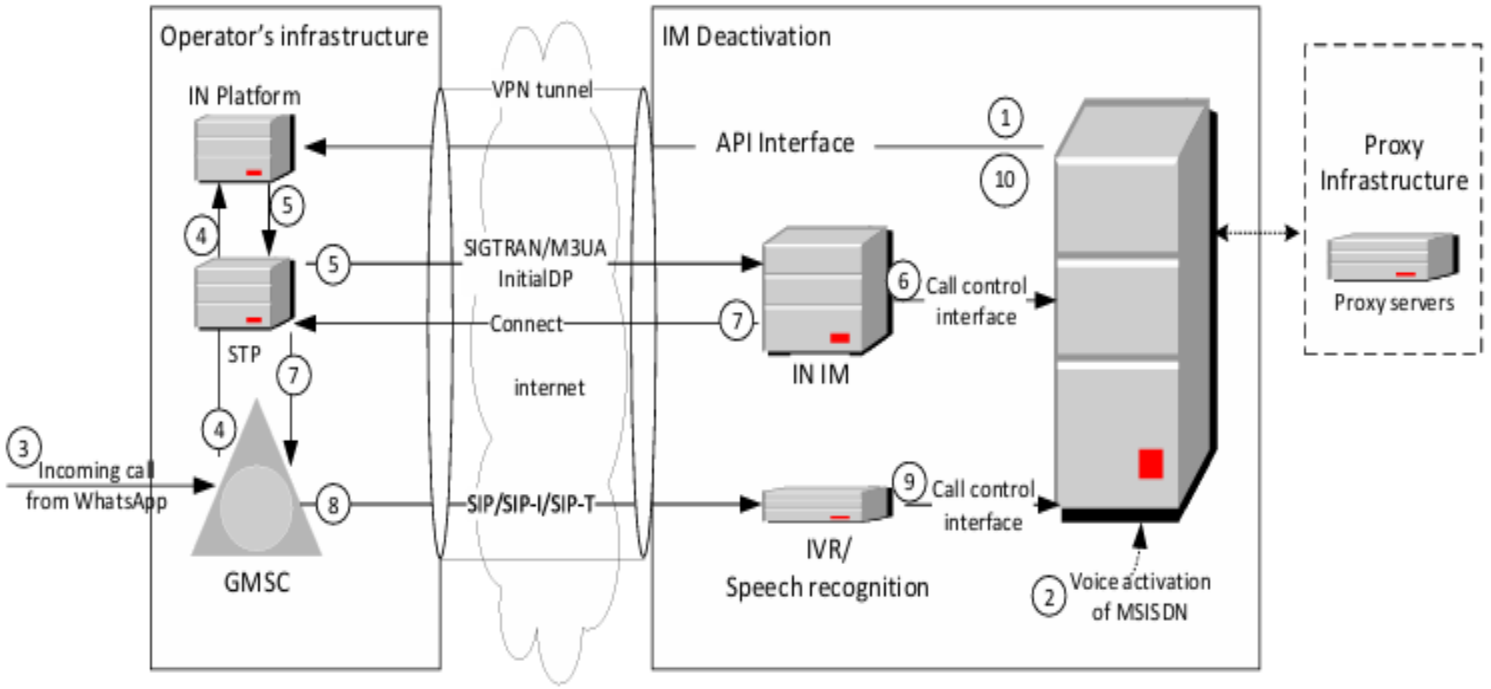



**Figure 6 Voice integration diagram**

**Дараах байдлаар ажиллана:**

1.IM Deactivation шийдэл нь идэвхгүй болгох MSISDN-ийг сонгож, API интерфэйсээр дамжуулан IN платформд CAMEL чиглэл өөрчлөлтийн тохиргоо хийнэ.

2.IM Deactivation шийдэл нь OTP-г дуудлагаар хүлээн авах процессыг эхлүүлнэ.

3.WhatsApp эсвэл Telegram-аас ирж буй дуудлага операторын GMSC-д дамжуулна.

4.GMSC нь CAMEL InitialDP мессежийг операторын IN платформ руу илгээнэ.

5.IN платформ нь InitialDP мессежийг IN IM модуль руу дамжуулна.

6.IN IM модуль нь OTP-г хэрхэн боловсруулах (А дугаараас авах эсвэл дуу таних аргаар авах) зааврыг авахын тулд IM Deactivation шийдэлд хүсэлт илгээнэ.

7.IM Deactivation шийдэл нь дуудлагыг цаашид боловсруулахын тулд (В дугаарт урьдчилсан код нэмэн) IVR сервер рүү чиглүүлнэ.

8.IVR систем нь 6-р алхмаар авсан мэдээлэлд тулгуурлан дуу таних үйлдэл хийж эсвэл дуудлага холбогдох дохио тоглуулж, OTP-г хүлээн авна.

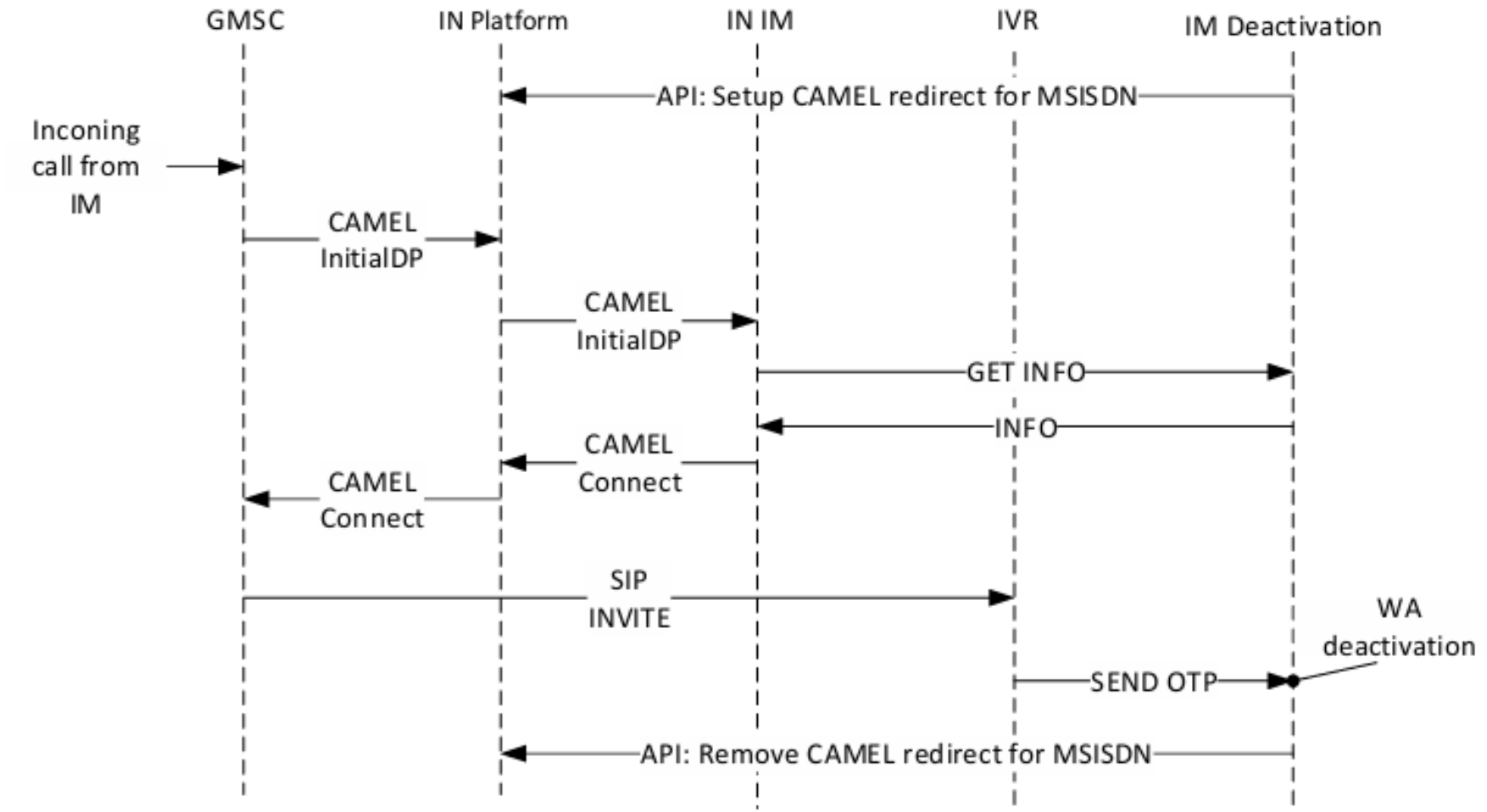
9.IVR систем нь OTP-г IM Deactivation шийдэл рүү илгээн устгах үйл явцыг дуусгана.

10.IM Deactivation шийдэл сонгосон MSISDN-ийг IN платформоос устгана.

# IM DEACTIVATION SOLUTION REQUIREMENTS FOR POC, MONGOLIA

## САНАЛ БОЛГОЖ БУЙ PROOF-OF-CONCEPT VOICE INTEGRATION

Messages flow

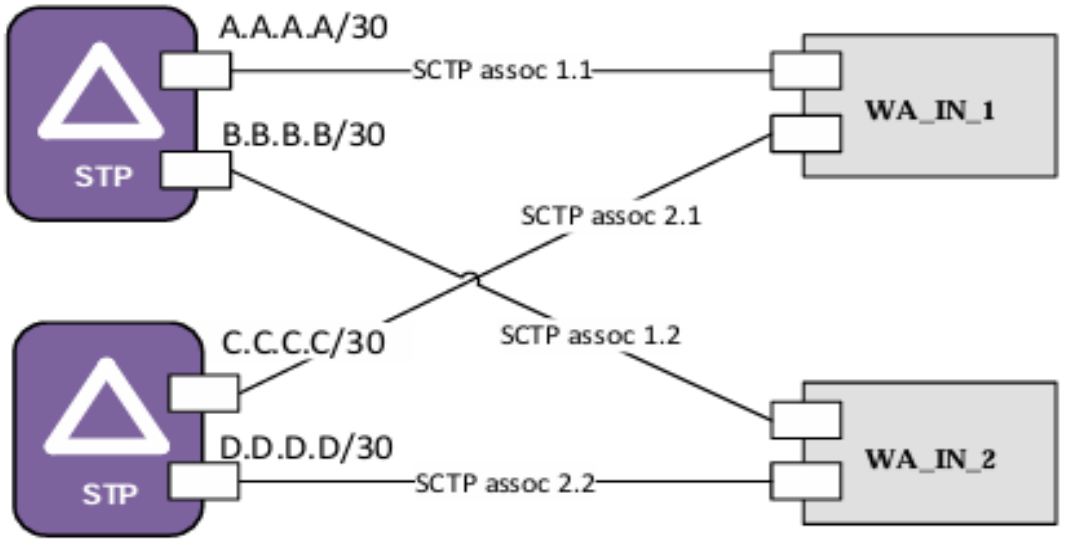


# IM DEACTIVATION SOLUTION REQUIREMENTS FOR POC, MONGOLIA

## САНАЛ БОЛГОЖ БУЙ PROOF-OF-CONCEPT INTERFACE

**SCTP интерфэйс нь i**nitial DP мессежийг хүлээн авахдаа WhatsApp эсвэл Telegram-аас дуудлагыг IVR систем рүү шилжүүлэхэд ашигладаг.

**Transport protocol stack**: IP/SCTP/SIGTRAN/M3UA




**SIP/SIP-T/SIP-T интерфейс:**

SIP/SIP-I/SIP-T интерфэйс нь дуут **дуудлагыг чиглүүлэх** энгийн SIP trunk-ийг төлөөлдөг.

**Дуудлагын хяналтын интерфейс:**

Дуудлагын хяналтын интерфэйс нь **IN IM** болон **IM** идэвхгүйжүүлэх модулийн хоорондох **модуль хоорондын протоколыг төлөөлдөг**.

**API интерфейс:**

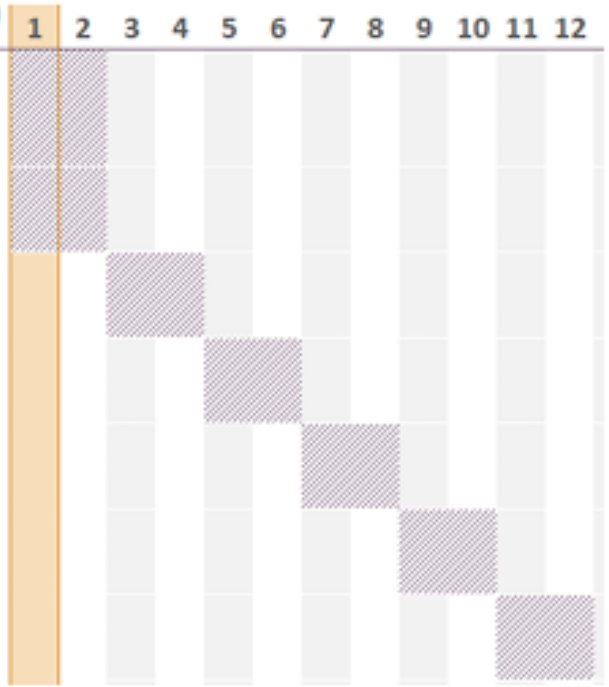
API интерфэйс нь тусгай MSISDN-д зориулсан InitialDP мессежийг IM идэвхгүй болгоход чиглүүлэх зорилгоор операторын IN платформ дээр хэрэгжсэн интерфейс юм. Хэрэв IN платформ нь API интерфейсийг дэмждэггүй бол техникийн шийдлийг операторын чадварт тохируулж болно.

POC дээр зөвхөн нэг SCTP холбоо байгуулна = туршилтад нэг сувгаар сигналыг дамжуулж шалгана, харин production дээр олон сувгаар найдвартай ажиллагааг хангана.

# IM DEACTIVATION SOLUTION REQUIREMENTS FOR POC, MONGOLIA

## САНАЛ БОЛГОЖ БУЙ PROOF-OF-CONCEPT POC IMPLEMENTATION PLAN

| ACTIVITY | RESPONSIBLE | PLAN START (WEEK #) | PLAN DURATION (WEEKS) |
|---|---|---|---|
| Discuss and approve POC technical solution | Reguklator,Mobile oerator, Hexagon Labs | 1 | 2 |
| Deploy a small prototype of the system at Hexagon Labs. | Hexagon Labs | 1 | 2 |
| Perform SMS integration | Hexagon Labs, Mobile operator | 3 | 2 |
| SMS integration tests | Hexagon Labs, Mobile operator | 5 | 2 |
| Perform Voice integration | Hexagon Labs, Mobile operator | 7 | 2 |
| Voice integration tests | Hexagon Labs, Mobile operator | 9 | 2 |
| POC Evaluation | Reguklator,Mobile oerator, Hexagon Labs | 11 | 2 |

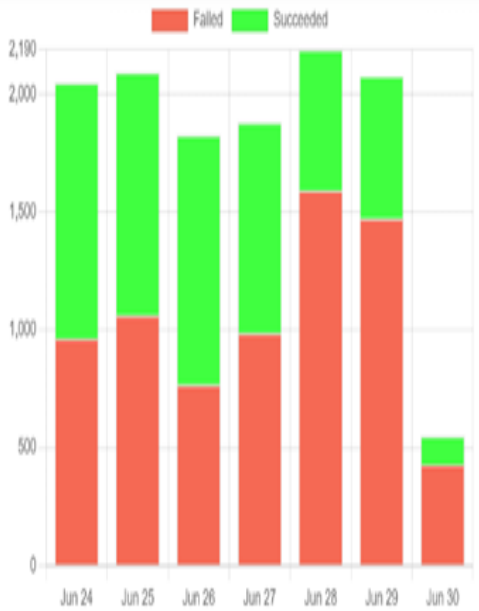


# IM DEACTIVATION SOLUTION REQUIREMENTS FOR POC, MONGOLIA

## САНАЛ БОЛГОЖ БУЙ PROOF-OF-CONCEPT REPORTING

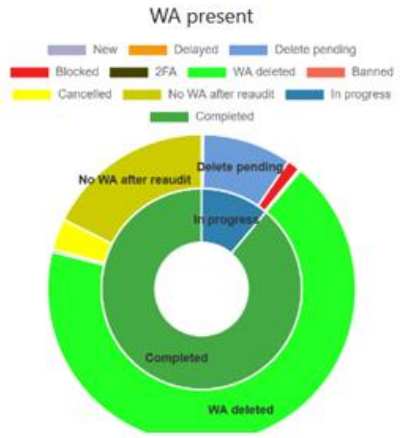
Энэхүү шийдэл нь график болон хүснэгтийн аль алинд нь ашиглах боломжтой тайлан, статистикийг гаргах вэб дээр суурилсан интерфейсийг агуулдаг.График дүрслэлийг өдөр тутмын явцын тайлан, ерөнхий үр дүн, оролтын өгөгдлийн тайланд зориулж хэрэгжүүлдэг.

| Date | Total | Succeeded | Failed |
|---|---|---|---|
| Jun 24 | 2048 | 1084 | 964 |
| Jun 25 | 2092 | 1030 | 1062 |
| Jun 26 | 1826 | 1059 | 767 |
| Jun 27 | 1880 | 894 | 986 |
| Jun 28 | 2189 | 598 | 1591 |
| Jun 29 | 2077 | 604 | 1473 |
| Jun 30 | 548 | 119 | 429 |




Full Numbers Statistics

| Category | Count | %% |
|---|---|---|
| **Total** | 1725156 | 100 % |
| **Audit pending** | 0 | 0 % |
| **Audited** | 1725156 | 100 % |
| WA present | 557046 | 32.3 % |
| WA absent | 1168110 | 67.7 % |
| **Completed** | 495207 | 28.7 % |
| WA deleted | 377542 | 76.2 % |
| Banned | 1599 | 0.3 % |
| Cancelled | 18186 | 3.7 % |
| No WA after reaudit | 97880 | 19.8 % |
| **In progress** | 61841 | 3.6 % |
| New | 26 | 0.0 % |
| Delayed | 1217 | 2.0 % |
| Delete pending | 51972 | 84.0 % |
| Blocked | 7398 | 12.0 % |
| 2FA | 1228 | 2.0 % |

# POC FOR NATIONAL ANTI-FRAUD SOLUTION MONGOLIA

## Hexagon Labs-ийн NAS шийдэл (Монголд санал болгосон)

•**Төвлөрсөн бүрэлдэхүүн**:

- **Central Management & Monitoring System (CMMS)**
- **Verification Exchange Hub** – операторуудыг нэг backbone-аар холбож, мэдээллийг real-time дамжуулах.

•**Тархсан бүрэлдэхүүн**:

- **Verification Nodes** – оператор тус бүр дээр байрлаж дуудлага/SMS шалгаж, query-д хариу өгөх

•**Үйл ажиллагааны зарчим:** Out-of-band verification (HTTP/JSON, SS7), бодит цагийн CLI шалгалт, баталгаажуулалтгүй дуудлагыг таслах.

## Hexagon Labs-ийн IM Deactivation POC

•**Төвлөрсөн бүрэлдэхүүн**:

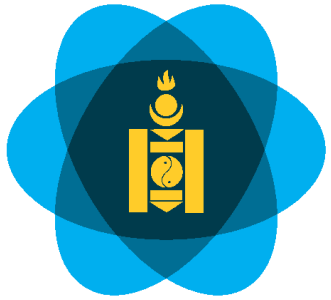
•MSISDN (Mobile Station International Subscriber Directory Number-**E.164 стандарт** дээр суурилагдсан олон улсын форматтай гар утасны хэрэглэгчийн бүрэн дугаар) blacklist/registry, админ удирдлага.

•IM Deactivation нь OTP-г ашиглан тухайн **аккаунтыг автоматаар идэвхгүйжүүлнэ**

•**Тархсан бүрэлдэхүүн**:

- Distributed Android farm + Proxy infra (үйлдлийг тархсан байдлаар автоматжуулж хэрэгжүүлдэг).

**IM Deactivation** бол дэмжих туслах шийдэл бөгөөд гол backbone биш, харин **тархсан түвшинд complement шийдэл** болж өгнө.



ХАРИЛЦАА ХОЛБООНЫ
ЗОХИЦУУЛАХ
ХОРОО


# Анхаарал хандуулсанд баярлалаа.