ITUWebinars

# Signalling Security

*Episode 2:*
*Securing legacy telecom network services*

7 November 2022
15:00-17:00, CET

https://itu.int/go/WB-SSP-02

Assaf Klinger, SG11

# Agenda

- Overview of legacy telecom services and their main use cases
- Current security issues in legacy telecom services
- Best-practice security mitigations for these attacks which do not require major infrastructure spend and their limitations
- Use cases for applying best practices for improving legacy telecom services security

# A little about myself

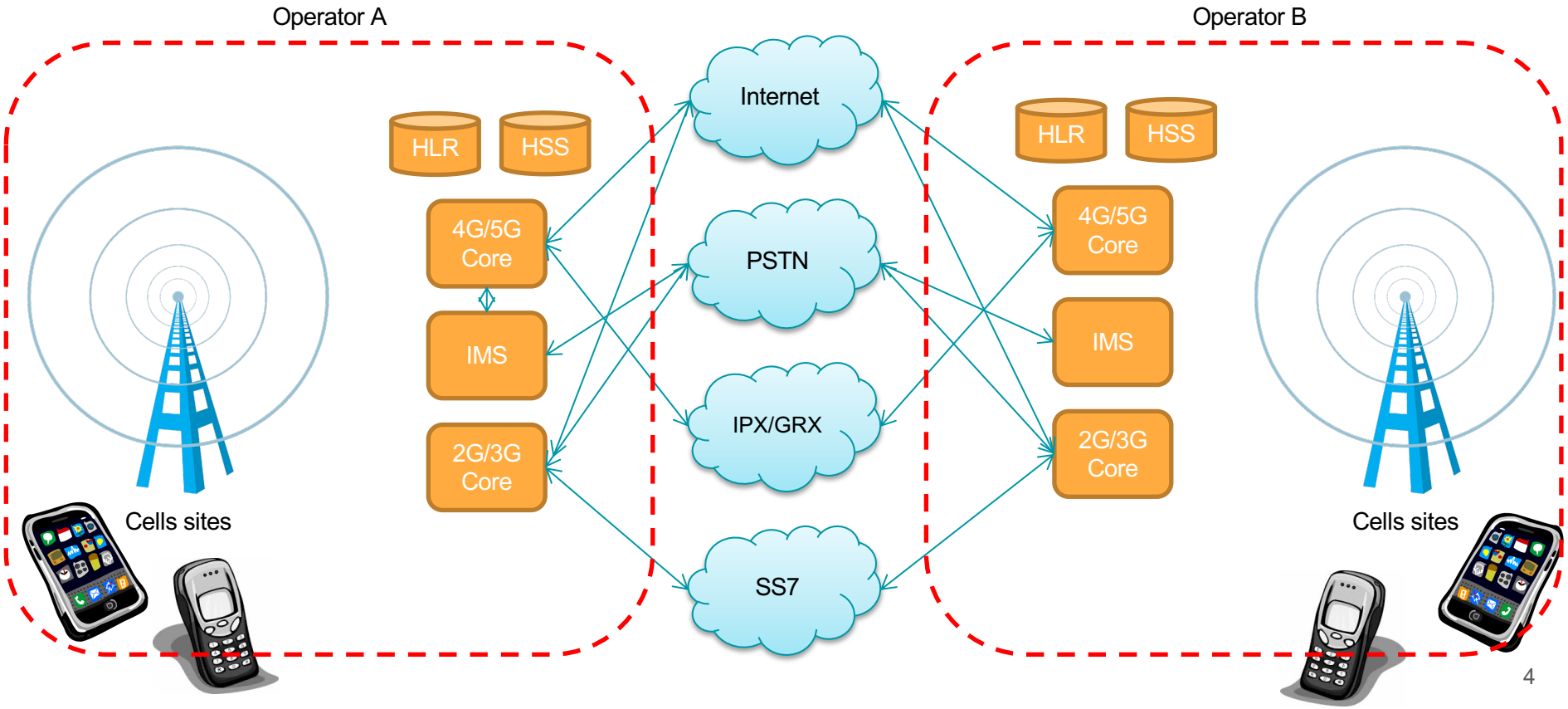
- Husband, father (+2), geek 8-)
- Security researcher for the last 18 years
  - Specialize in telecom, IoT & blockchain
  - Editor of ITU-T Study Group 11 recommendations
  - Member of FIGI SIT WG & DFGI SA WG
- Handles:


Assaf.klinger@gmail.com

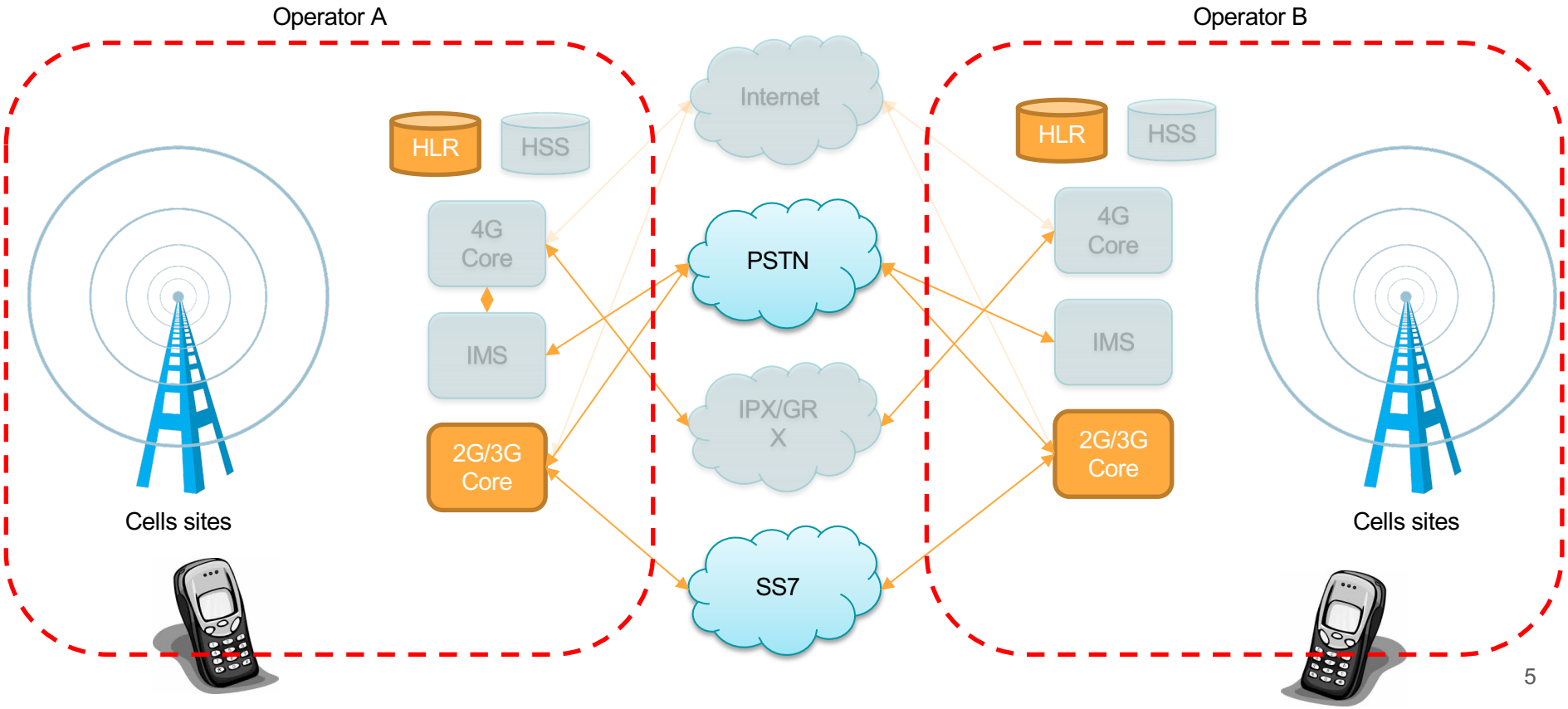
@AssafKlinger

https://www.linkedin.com/in/assaf-klinger-8a0b7159/

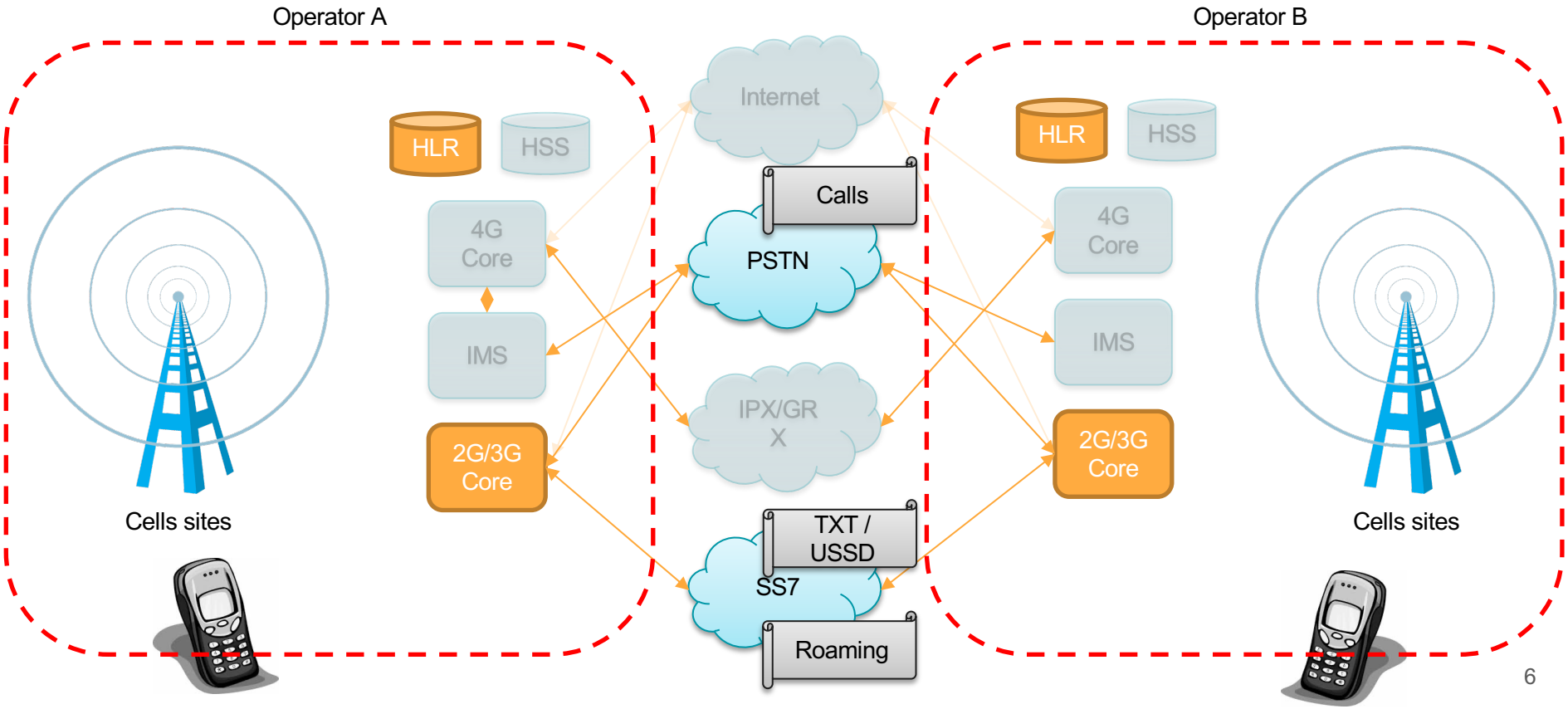

# Telco's core network (very high level)



# Today we're discussing legacy networks



# Telecom services provided by legacy network



# Legacy services main use-cases

- 2G/3G networks are very common in rural areas and are still in use for:

| Service / UC | Banking | Communication | Authentication |
|---|---|---|---|
| SMS | ✓ | ✓ | ✓ |
| USSD | ✓ | × | × |
| Voice Call | × | ✓ | ✓ |

- 2G/3G networks are still active because:
  - LTE / 5G have 20% of the range a GSM cell has
  - No data coverage is needed where feature-phones are dominant
  - Shutting down 2G/3G requires a total upgrade of the core network

**Telcos won’t invest in infrastructure if they don’t have to**

# Legacy networks are far more vulnerable than modern networks

| Network Generation | Intercept | | Impersonation | | Tracking | | DoS | |
|---|---|---|---|---|---|---|---|---|
| | Local | Remote | Local | Remote | Local | Remote | User | Network |
| 5G | ○ | ○ | ○ | ○ | ○ | ○ | ◐ | ◐ |
| 4G | ○ | ◔ | ◑ | ○ | ● | ◑ | ● | ● |
| 3G | ○ | ● | ◑ | ● | ● | ● | ● | ● |
| 2G | ◔ | ● | ● | ● | ● | ● | ● | ● |

5G standards can potentially reduce security risks in all dimensions

○ Less risk
● More risk

Source: SR Labs telco hacking toolbox

# Major attacks on legacy network in the wild

Caller ID spoofing


2FA account takeover

Geo Location

# 2FA SMS interception via SS7 attack

Example

Log in to your PayPal account

paypal.com/il/si...

Incognito

PayPal

Email or mobile number

Next

or

Sign Up

Privacy Legal



Consumer advisory - PayPal Pte. Ltd., the holder of PayPal's stored value facility, does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully.

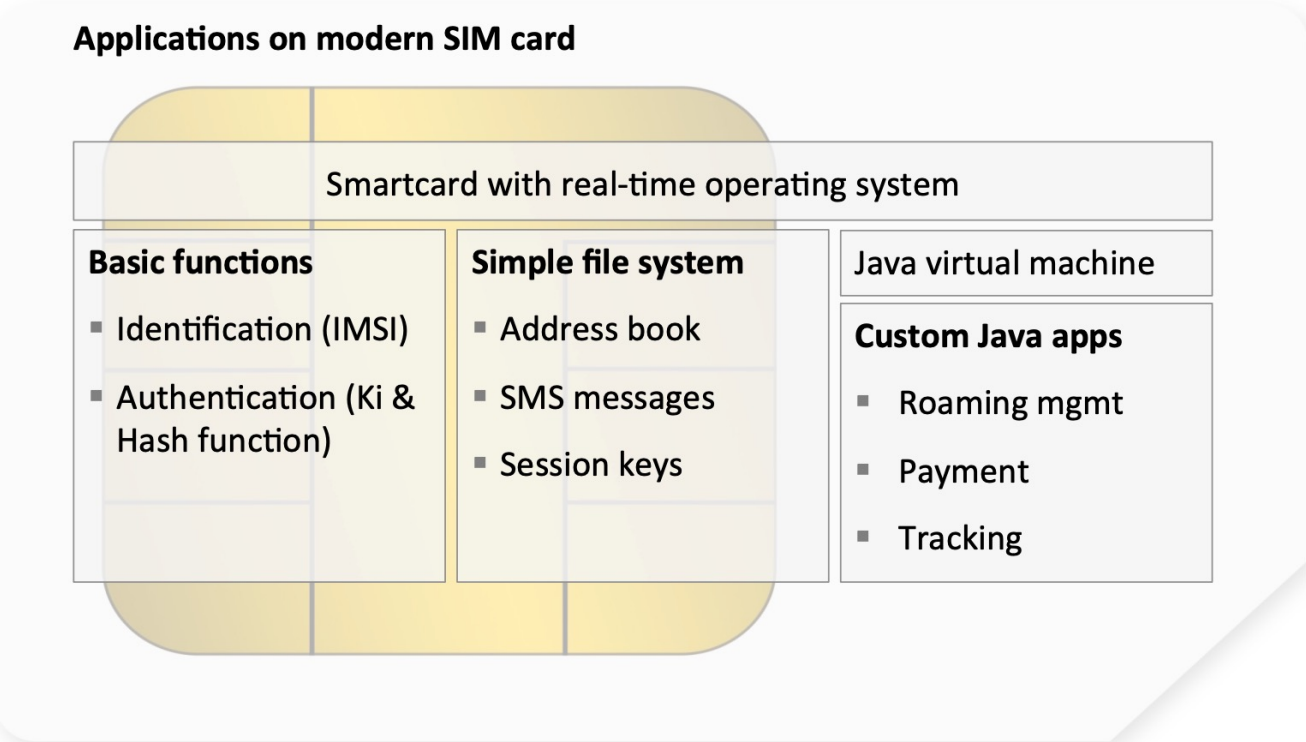
assaf@DESKTOP-MCKINNK: /mnt/c/Work/Vaulto/Vaulto/tests

```
assaf@DESKTOP-MCKINNK:~$ cd /mnt/c/Work/Vaulto/Vaulto/tests/
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ clear
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ python demo_ul_sms_intercept.py 972502138133 new
```

# Attacking SIM cards via OTA messages (“binary SMS”)

Example

# SIM cards are fully programmable computer systems




**ISO/IEC 7816 Smart card (Universal Integrated Circuit Card - UICC)**

# SIM cards in legacy networks

| Application | 2G - SIM | 3G - SIM+uSIM | 4G - SIM+uSIM+iSIM |
|---|---|---|---|
| Smart Card type | ICC | UICC | UICC / eUICC |
| CPU | 8bit | 16bit | 32bit |
| Storage ($E^2$PROM) | Up to 32 Kbyte | Up to 128 KByte | Up to 256 Kbyte |
| Interface | Electrical | Electrical | Electrical / NFC |
| # of identities | 1 | 2 | multiple |
| OTA authentication | DES | 3DES | AES |

DES & 3DES are **broken** authentication schemes!!

# A Java virus on the SIM card has access to lots of abusable functionality

| OTA-deployed SIM virus can access SIM Toolkit API | |
|---|---|
| **Standard STK function** | **Abuse potential** |
| **Send SMS** | ▪ Premium SMS fraud |
| **Dial phone numbers, send DTMF tones** | ▪ Circumvent caller-ID checks<br>▪ Mess with voice mail |
| **Send USSD numbers** | ▪ Redirect incoming calls; sometimes also SMS<br>▪ Abuse USSD-based payment schemes |
| **Query phone location and settings** | ▪ Track victim |
| **Open URL in phone browser** | ▪ Phishing<br>▪ Malware deployment to phone<br>▪ Any other browser-based attack |

# Best-practice security mitigations

# Mitigating SS7 attacks

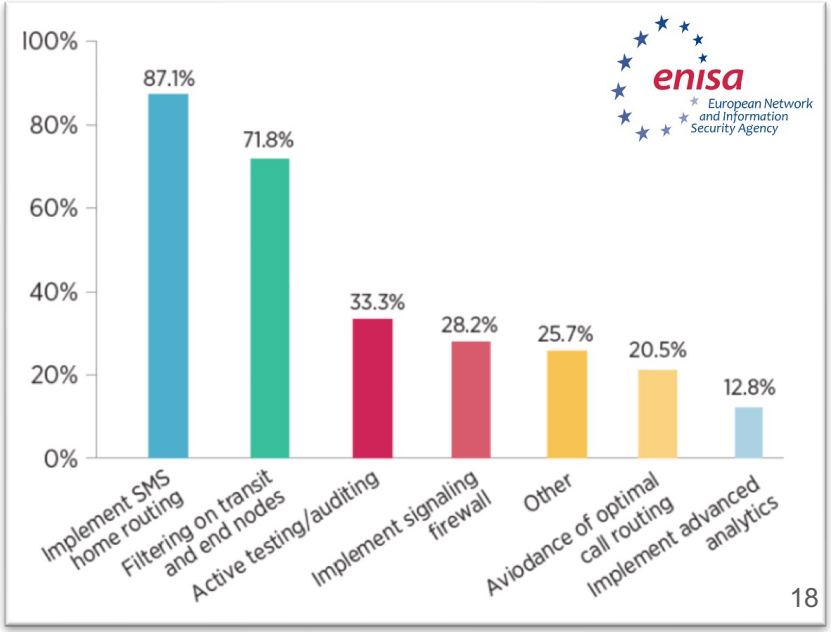
- Implementation of configuration recommendations

| Attack | FS.11 (2/3G) | FS.07 (2/3G) | IR.82 (2/3G) | IR.88 (4G) |
|---|---|---|---|---|
| Spoofing | ✓ | ✓ | ✓ | × |
| SMS Hijack | × | ✓ | × | × |
| Geo Location | × | ✓ | ✓ | ✓ |

- Commercial signaling firewalls
  - Stateless vs. stateful
  - Threat intelligence

# Limitations of available mitigation measures

- Implementation of configuration recommendations
  - Doesn't solve attacks using legitimate signaling flows
  - Low adoption by operators
- Commercial signaling firewalls
  - Low adoption by operators
  - Threat intelligence depends on attack information sharing between operators



# Mitigating SIM cards attacks (via OTA)

Low High

| Mitigation layer for OTA hacking risk | Effectiveness | Cost | |
|---|---|---|---|
| Filter OTA messages from unapproved sources | Prevents probing in home network; leaves SIMs exposed when roaming, to fake base stations, and to phone malware | Functionality readily available in most SMSCs | Network operators short-term mitigation option |
| Deactivate OTA on card | Prevents attack (but also any future use of OTA w/ DES key) | Can be done through SMS | |
| Use 3DES or AES OTA keys | Prevents attack (expect for where downgrade attack works) | Some cards need replacing, others updates | Network operators mid-term mitigation option |
| Use cards that do not disclose crypto texts | Prevents the attack | Some cards need to be replaced | |
| Filter suspicious messages on phone base band | Prevents the attack | New software function for future phones | Complimentary mitigation option for phone manufacturers |

# Mitigation Measures for non-operators

- Change the direction of 2FA

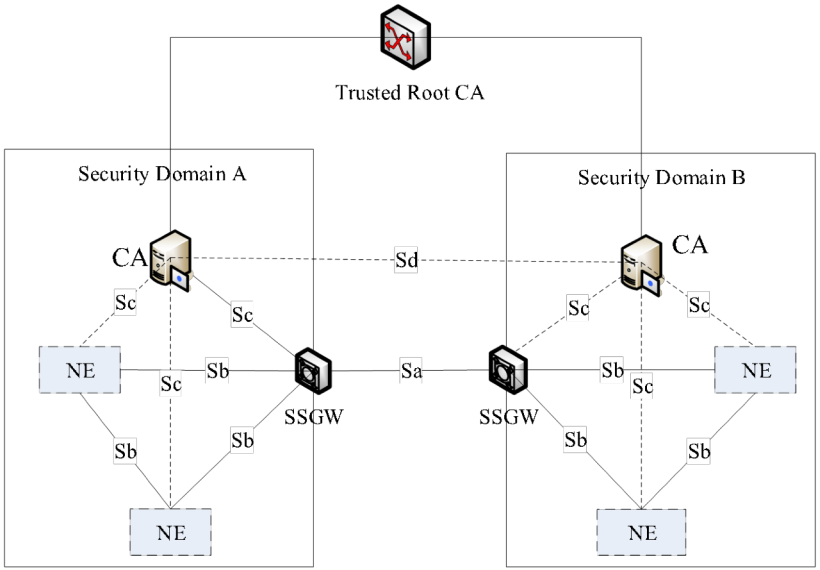
- Use a SIM Validation gateway

# The solution to the problem is already here

- Adding an integrity layer to signaling transactions to enable trustable communications
- Some example of applications:
  - Calling Line Identification (CLI) authentication
  - 2FA
  - Digital Financial Services (DFS)
  - And more…

# Implement ITU-T SG11 recommendations

- ITU-T Q.3057 and ITU-T Q.3062
  - Adds digital signature to SS7 signaling to authenticate the sender
  - Prevents hackers from impersonating legitimate network functions on the SS7 network
  - Enables operators to manage trust of other operators
  - Using TLS 1.3 as a reference trust model
- ITU-T Q.3063
  - Uses *Q.3057* and *Q.3062* as infrastructure for CLI authentication
  - Uses authentication tokens to prevent CLI spoofing



# But what about the trust model?

## Trust model

- We will need to build a hierarchy of trust, country/regional first, then global. where each local regulator will have to determine how to implement the certification depending on their local forms of identification and rules
- **Technically the digital certificates must be interoperable across domains** (SIP, SS7 and others).
- This trust chain and certification standard must account for the fact that numbering is no longer geographical and different authorities can govern the same numbering range
- **The trust anchor needs to be a globally trusted SDO**, preferably one already in charge of numbering and this anchor must interoperate with existing repositories (such as the ones in the US and Canada)

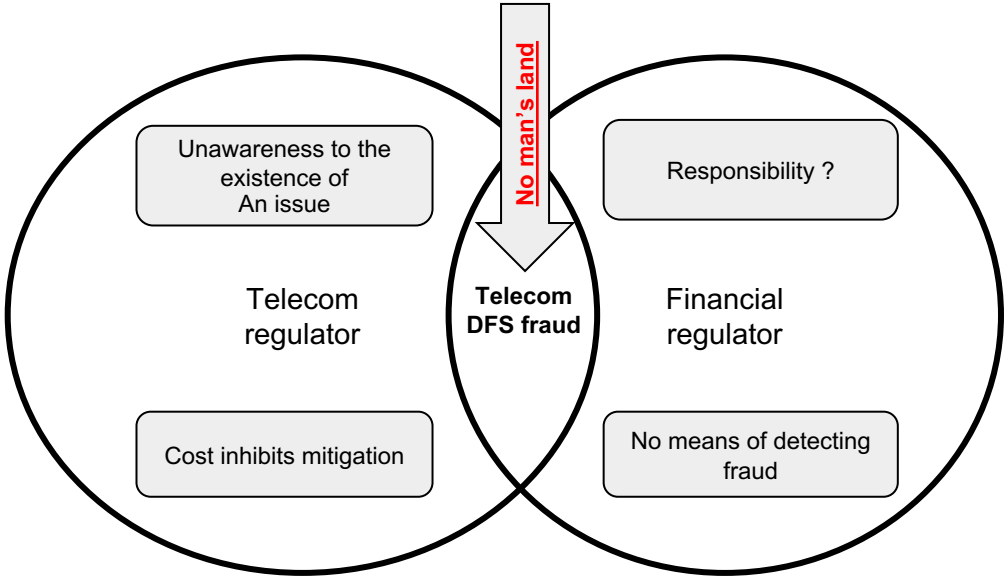
## vetting/certification process

- **We will need to formulate a way to standardize these local/regional certification processes** in order to keep the bad actors out. This standardization process should involve as many counties as possible in order to improve its applicability on the global scale
- The certification process implemented in the US and Canada for STIR/SHAKEN is a good use case to learn from in order to standardize it on the global scale
- These certification process standardization must be connected to a largely accepted digital identity management frameworks for the operator plane and for the individual plane

# Example for applying best practices

# Uganda

- Legislation of laws enabling fraud information sharing between financial and telecom sectors and establishment of a regulatory round–table
- Implementation of recommendations for the prevention of telecom attacks across all national operators



# Zimbabwe

- Registration of IMEI with the DFS provider when opening an account (simple MMI code)
- Mitigate SIM swap / SIM recycle by requesting IMEI information from the mobile operator via the USSD gateway and comparing to the registered IMEI
- When changing mobile phones, a new IMEI must be registered with the DFS provider using proof of identity (not over SMS)

# Q&A


Assaf.klinger@gmail.com

@AssafKlinger

https://www.linkedin.com/in/assaf-klinger-8a0b7159/