Fourth ITU Regional Workshop for Africa
“Strengthening ICT Integrity: Combating Counterfeits, Testing Challenges, and Fraudulent Communications in Africa Region”
Tunis, Tunisia, 1 October 2025

SESSION 3: COMBATING FRAUDULENT COMMUNICATIONS IN THE REGION

Mobile Technical Fraud
IMEI (nternational Mobile Equipment Identity) Reprogramming

Hajer Tahri Beltaief
Senior IT Analyst
Head of Fraud Department in Tunisia Telecom

Summury

1. Definition
2. Modus Operandi
3. Types of Fraud Associated with Non-Approved Phones
4. Detection Method
5. Best Defence Mechanisms
6. Sajalni Platform (Tunisie Telecom)
7. SAJALNI Platform (Secure Access Operator)
8. SAJALNI Platform (Benefits)

Definition

- The IMEI (International Mobile Equipment Identity) is a unique number (15 digits) that identifies each mobile phone or GSM/4G/5G terminal.
- It is programmed in the internal memory of the device, generally at the level of the modem/baseband chip (the one which manages communication with the mobile network);
- Is used by operators and systems such as EIR/CEIR to recognize the terminal, for example to block it if it is stolen or if it is not approved;
- Usual structure: TAC (Type Allocation Code) + SNR (Serial Number) + (and sometimes) SV (version). The TAC indicates the model/manufacturer.

↳ Since the IMEI is in rewritable memory, it is technically possible (but illegal) to modify or clone the IMEI

↳ IMEI reprogramming is used to circumvent blacklisting of terminal equipment.

Modus Operandi

- Stolen / subsidised / blacklisted mobile terminals are obtained from Networks, Service Providers / Dealers / Customers or Criminals.

- Stolen / subsidised / blacklisted terminals are exported or re-chipped locally with new identities (new IMEI)

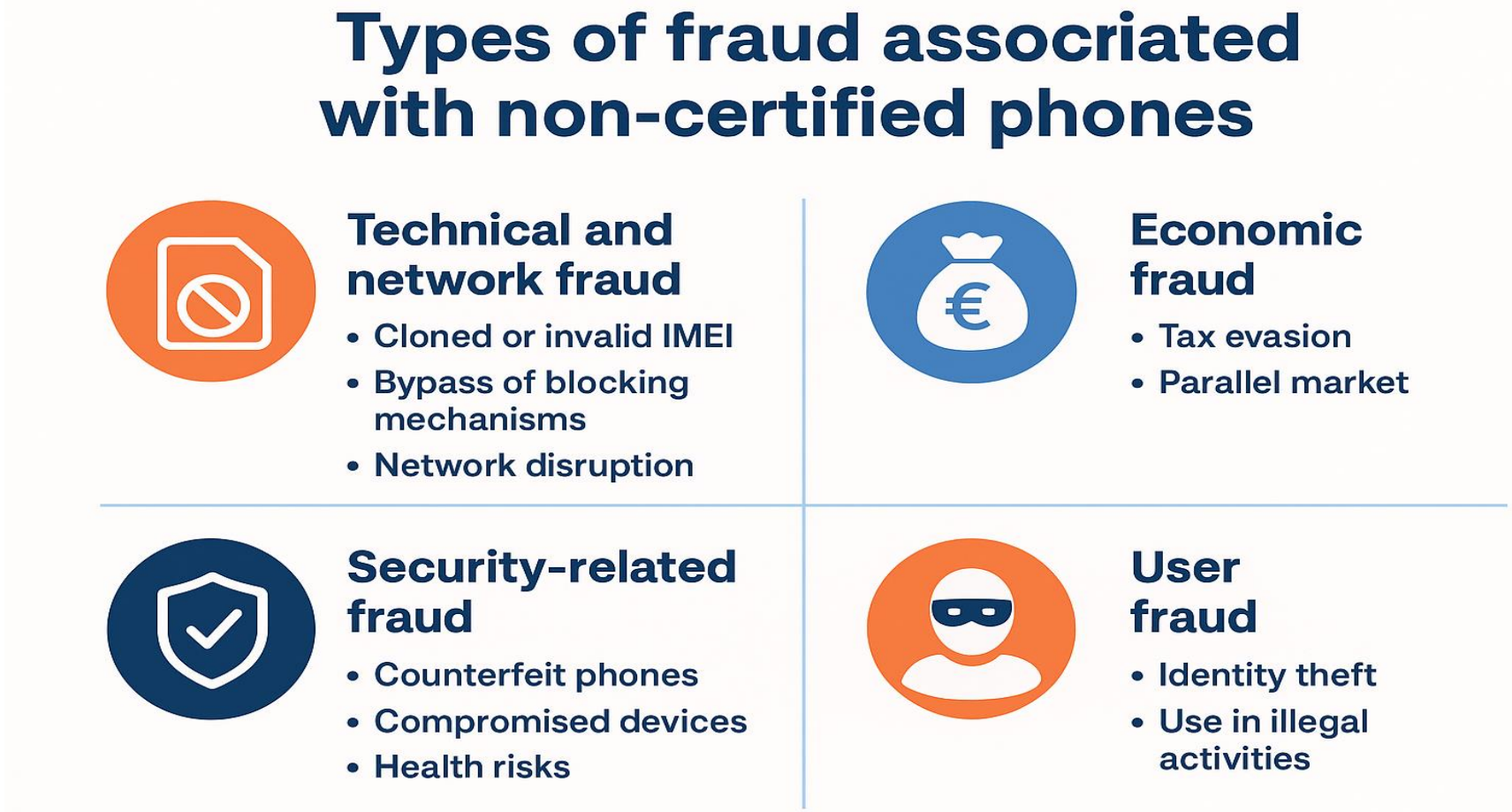
- **Re-c**hipping is carried out via:
  - ↳ Electronic reprogramming of the EEPROM (2G,3G)/Flash (smartphone) chip within the terminal
  - ↳ Physically replacing the EEPROM/Flash chip.

- Reprogrammed terminals with 'new' IMEIs are no longer SIM Locked or Blacklisted on the EIR (Equipment Identity Register) or CEIR (Central Equipment Identity Register)

- Reprogrammed terminals are then resold on the open market

❖ EEPROM (Electrically Erasable Programmable Read-Only Memory)

Types of Fraud Associated with Non-Approved Phones



Types of Fraud Associated with Non-Approved Phones

- Technical and Network Fraud
  - ↳Cloned or Invalid IMEI: The same IMEI can be duplicated on multiple devices → obscures traceability.
  - ↳ Bypassing blocking mechanisms (e.g., stolen phones put back into circulation with modified IMEIs).
  - ↳Network Disruption: Non-compliant devices can cause interference and degrade service quality.
- Economic Fraud
  - ↳ Tax Evasion: Phones introduced onto the market without paying customs duties and VAT.
  - ↳Parallel Market: Promotes smuggling and illegal sales.
- Security Fraud
  - ↳ Counterfeit phones or phones that do not comply with safety standards → risks to health (non-compliant waves) or electrical safety (overheating, fire).
  - ↳ Compromised Devices: Some non-approved phones may contain spyware or backdoors.
- User Fraud
  - ↳ Identity theft: Unauthorized devices can be used to bypass SIM/IMEI verification mechanisms.
  - ↳ Use in illegal activities: fraudulent international calls (SIMBOX, bypass), cybercrime, financial fraud.

Detection Method

- Phone may be badged with foreign network name/logo.
- Interior of phone shows signs of tampering.
- Multiple duplicate IMEIs appearing on fraud detection system.
- Multiple duplicate IMEIs appearing on EIR /CEIR
- TAC contained in the programmed IMEI does not conform to make/model of phone

Best Defence Mechanisms

- Identify duplicate IMEIs on EIR-CEIR / Network
- Identify Agent/dealer outlets selling/connecting this equipment.
- Notify customers and dealers that equipment does not satisfy type accreditation of network quality standards.
- Specify time period within which equipment should be replaced.
- Blacklist reprogrammed equipment.
- Issue warning to dealer that equipment does not comply with type accreditation.
- IMEI number range control via EIR/CEIR.
- Network handset purchasing strategy should be based on adherence to GSMA handset security requirements available from GSMA Security Group

SAJALNI Platform (Tunisie Telecom)

• SAJALNI application/service from Tunisie Telecom is a platform for controlling and approving mobile terminals (phones and tablets) since 2021

•It is an initiative launched by the Center for Telecommunications Studies and Research (CERT) in collaboration with Tunisie Telecom.

•The CERT maintains a blacklist of IMEIs numbers of phones that do not comply with standards or are reported stolen or fraudulent.

•This list is regularly updated to reflect newly prohibited devices.

↳Sajalni platform is twinned with that of the Association of Mobile Telephone Operators and Manufacturers (GSMA), thus making it possible to report stolen terminals and facilitate their blocking, even internationally

- Secure local operators access:

  ↳ Each operator such as Tunisie Telecom, Orange Tunisie, and Ooredoo has a secure account on the SAJALNI centralized platform

  ↳ They can consult the blacklist in real time or in batch mode to verify the IMEI when activating a device.

- Automatic or manual blocking:

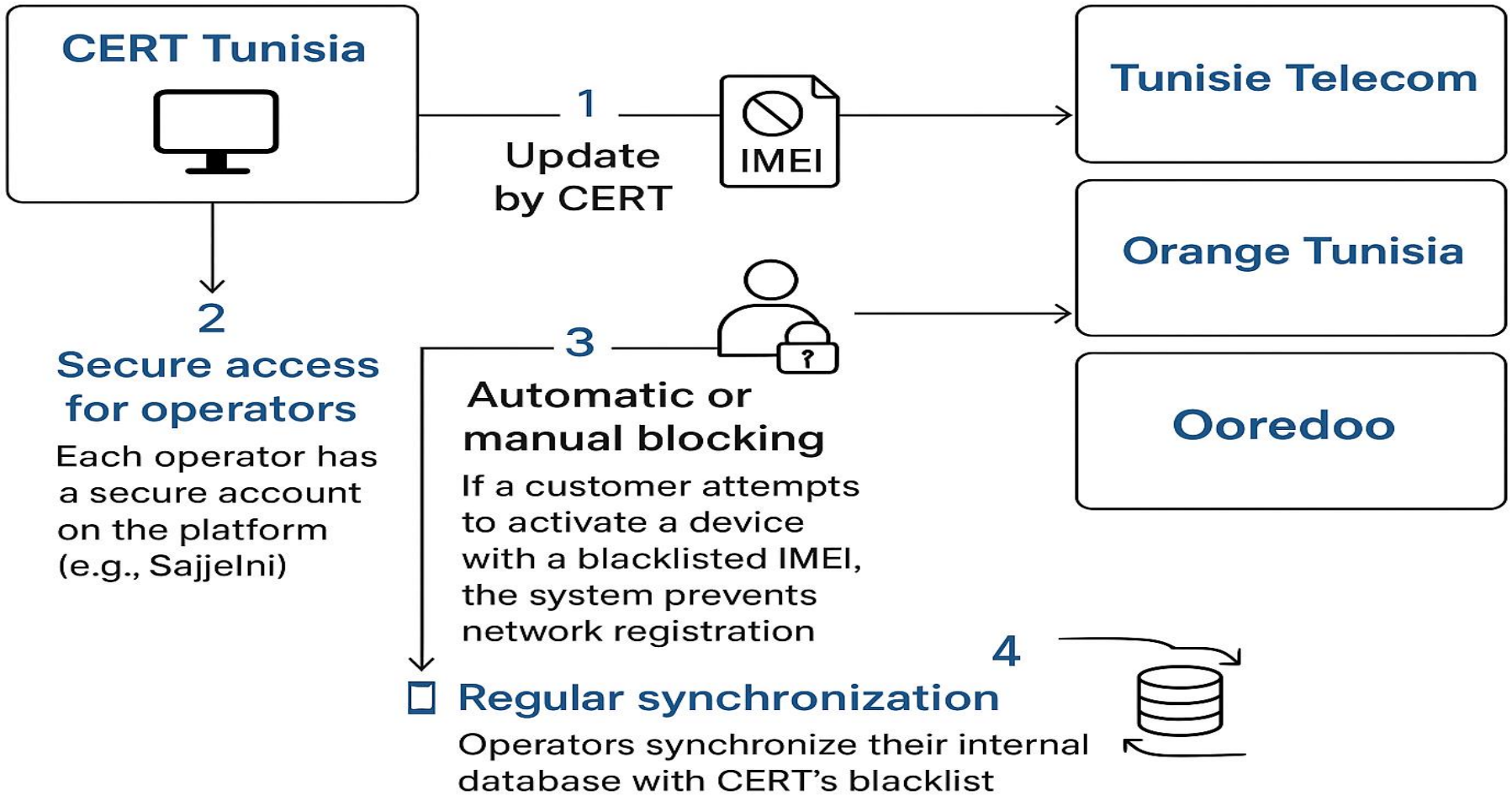
  ↳When a customer tries to activate a mobile phone whose IMEI is blacklisted, the operator's system prevents it from registering on the network.

  ↳ Operators can also detect these IMEIs during calls, text messages, or data usage, and automatically block the device

- Regular synchronization:

  ↳Operators regularly synchronize their own database with that of the CERT to ensure that no illegal devices go undetected.

SAJALNI Platform (Secure Access Operator)



Sajalni Platform (Benefits)

- Consumer protection against non-compliant devices.
- Reduction in the number of fraudulent/stolen devices in circulation
- Improved quality of service on the national network
- Contribution to the national economy by limiting illegal importation.

↳all non-compliant terminals may be blocked. If a user imports a terminal individually and inserts a local SIM card, they have a period (30 days) to register it, otherwise the terminal will be blocked

Thank You