Tunisian experience in combatting counterfeiting and stolen mobile devices using CEIR.

23-07-2018   Jamil Soyah

General context

- A population of about 11 million
- The mobile phone market in Tunisia records about 15 million mobile subscriptions
- A penetration rate of almost 128%
- Tunisia officially has 3 telecommunications operators and 1 MVNO
- Mobile phone market statistics show approximatively:
  - 7 million smartphones;
  - 2.5 Million new mobile phones are activated on Tunisian mobile networks every year including 1.5 Million smartphones.

- The counterfeit parallel market and theft of telecommunications terminal equipment or mobile devices have become global phenomena with serious economic and social consequences.
- The fight against these is more than ever relevant.
- In this context, the Tunisian State has decided to set up a central digital identification system for mobile terminals (Central Equipment Identity Register - CEIR) connecting to the Tunisian national telecommunications network.

Aims of CEIR-N

a. Collect data from all communication devices used in Tunisia and associate them with their users via the triplet: IMEI + IMSI + MSISDN

b. Filter devices or equipments or mobile communication terminals that are not allowed to operate in Tunisia:
   - counterfeit devices, or sub-standard devices
   - unapproved devices,
   - stolen and lost devices,

c. Create a global whitelist (ΔWLIMEI-CEIR-N) of the communication devices identified in (a);

d. Decline services to the communication devices referred to in point (b),

e. Continuous update (a) to (d) in real time

Expected earnings

- Strengthening Consumer Protection.
- Strengthening the implementation of the national strategy for the fight against corruption and tax evasion.
- Strengthening the application of the regulatory provisions on market control.
  Strengthening the Tunisian economy.
- Decrease:
  - the theft of mobile terminals,
  - the import of counterfeit mobile terminals,
  - the illegal importation of mobile terminals,
  - the marketing and use of mobile terminals that do not meet Tunisian technical specifications for interoperability and safety (electrical and health).
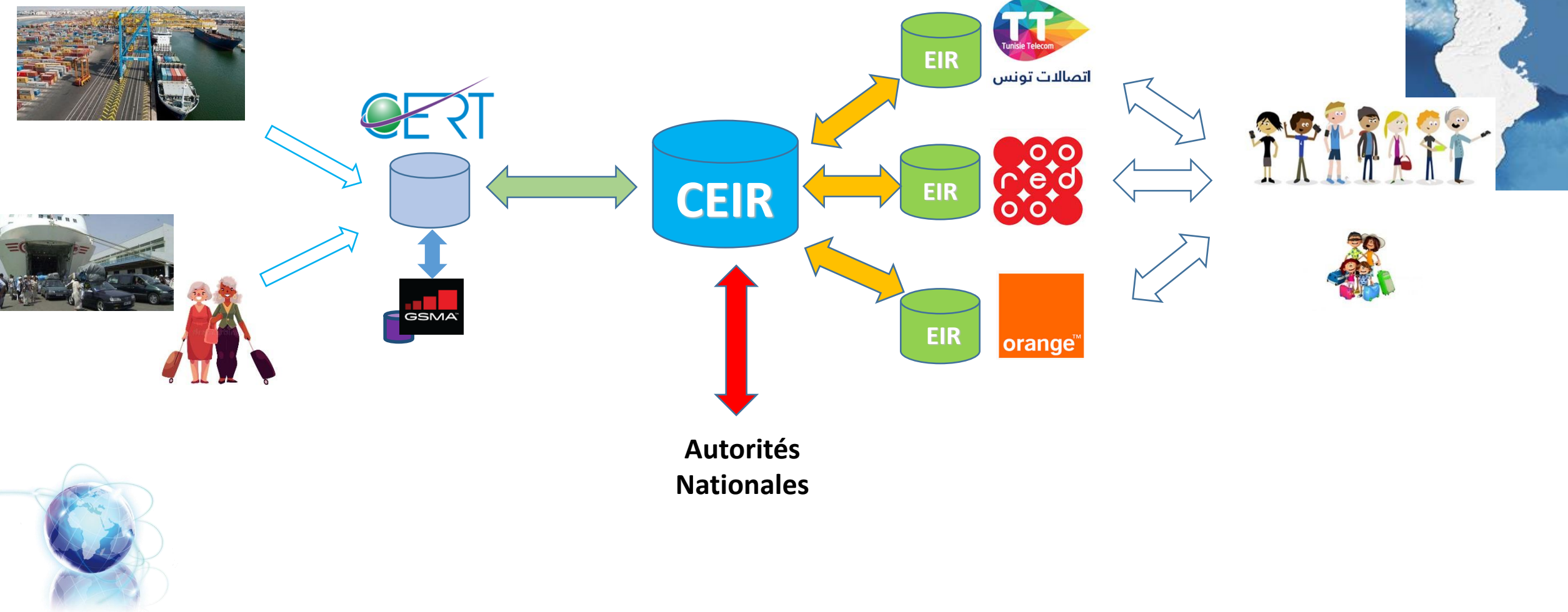
Stakeholders

- Lead : Ministry of Communication Technologies and Digital Economy
- Contracting Authority : Research and Studies Telecommunications Center
- Stakeholders:
  - National Instance of Telecommunications (National regulator)
  - National authorities
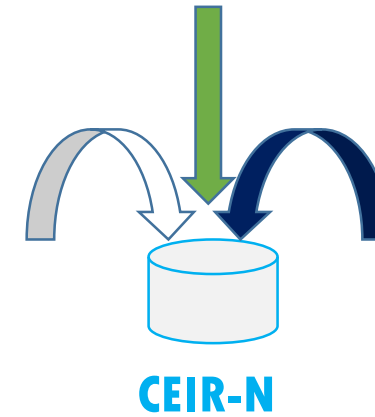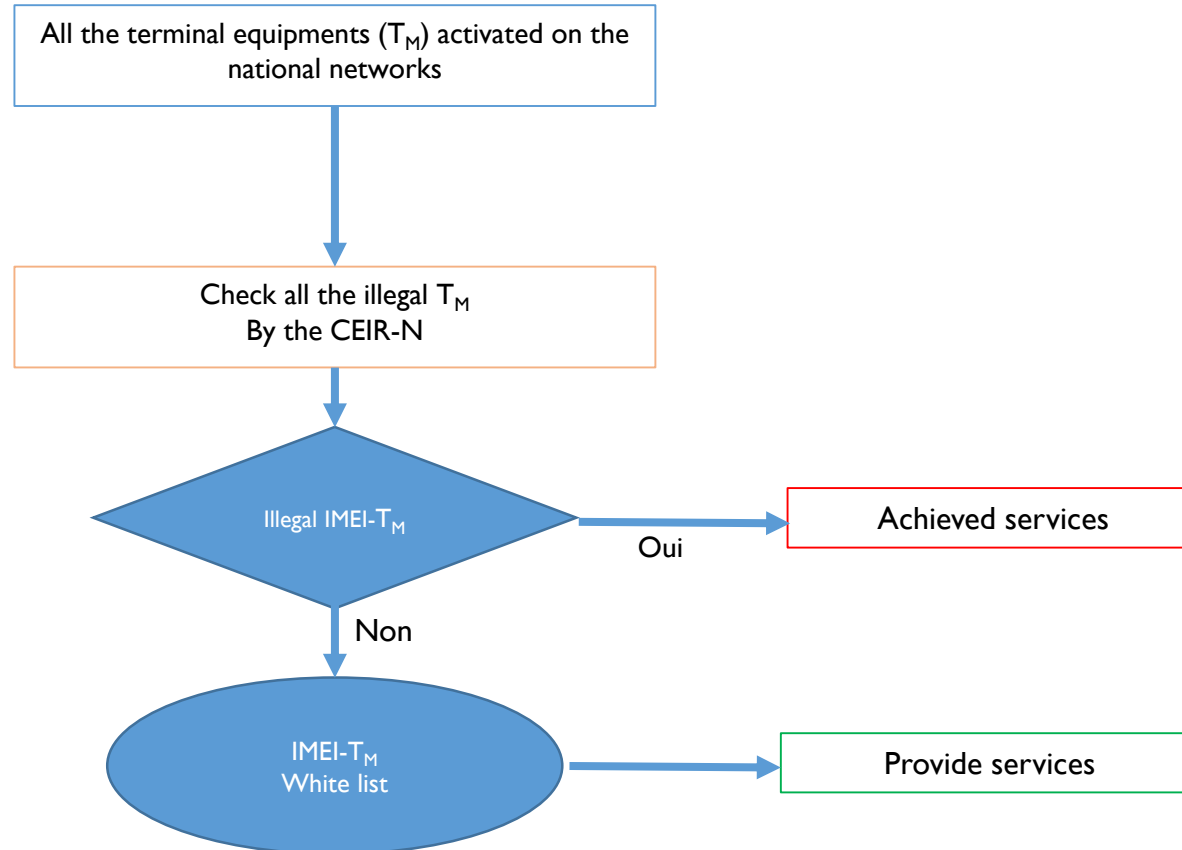 - Telecommunications operators
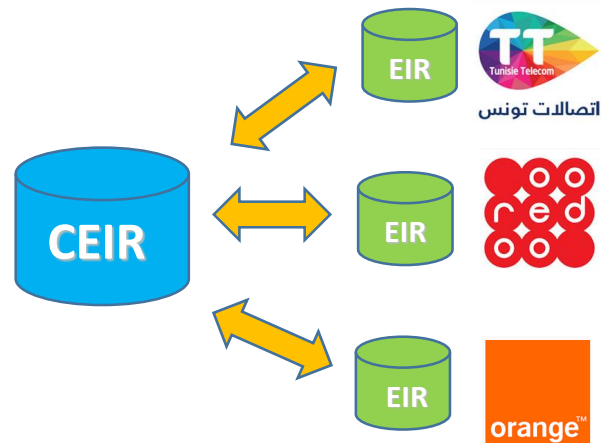
Target architecture

Description

The CEIR-N system is based on the establishment of a central database to register IMEIs of mobile terminals, spread over three lists:

- Whitelist
- Blacklist
- Temporary list

CEIR-N

```
┌─────────────────────────────────────┐
│ All the terminal equipments (T_M)    │
│ activated on the national networks   │
└─────────────────────────────────────┘
                  │
                  ▼
┌─────────────────────────────────────┐
│ Check all the illegal T_M            │
│ By the CEIR-N                        │
└─────────────────────────────────────┘
                  │
                  ▼
           ◇ Illegal IMEI-T_M ◇ ──Oui──▶ ┌──────────────────┐
                  │                        │ Achieved services │
                  │ Non                    └──────────────────┘
                  ▼
           ( IMEI-T_M          ) ─────────▶ ┌──────────────────┐
           ( White list        )            │ Provide services  │
                                            └──────────────────┘
```
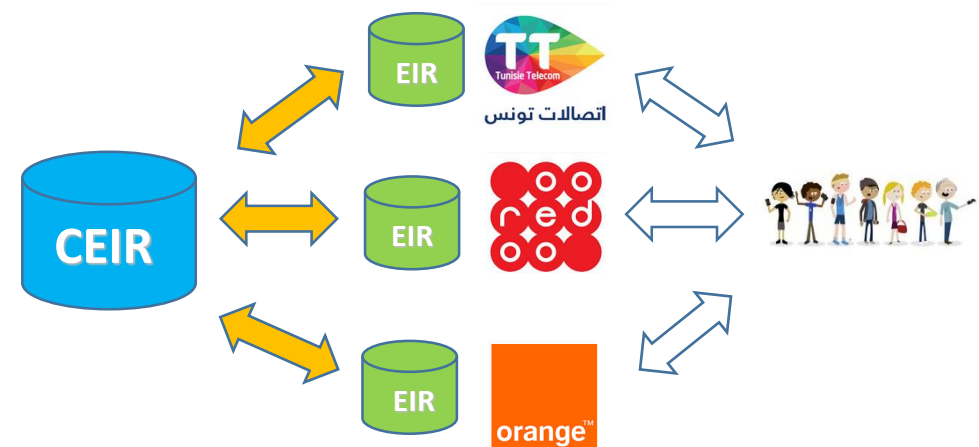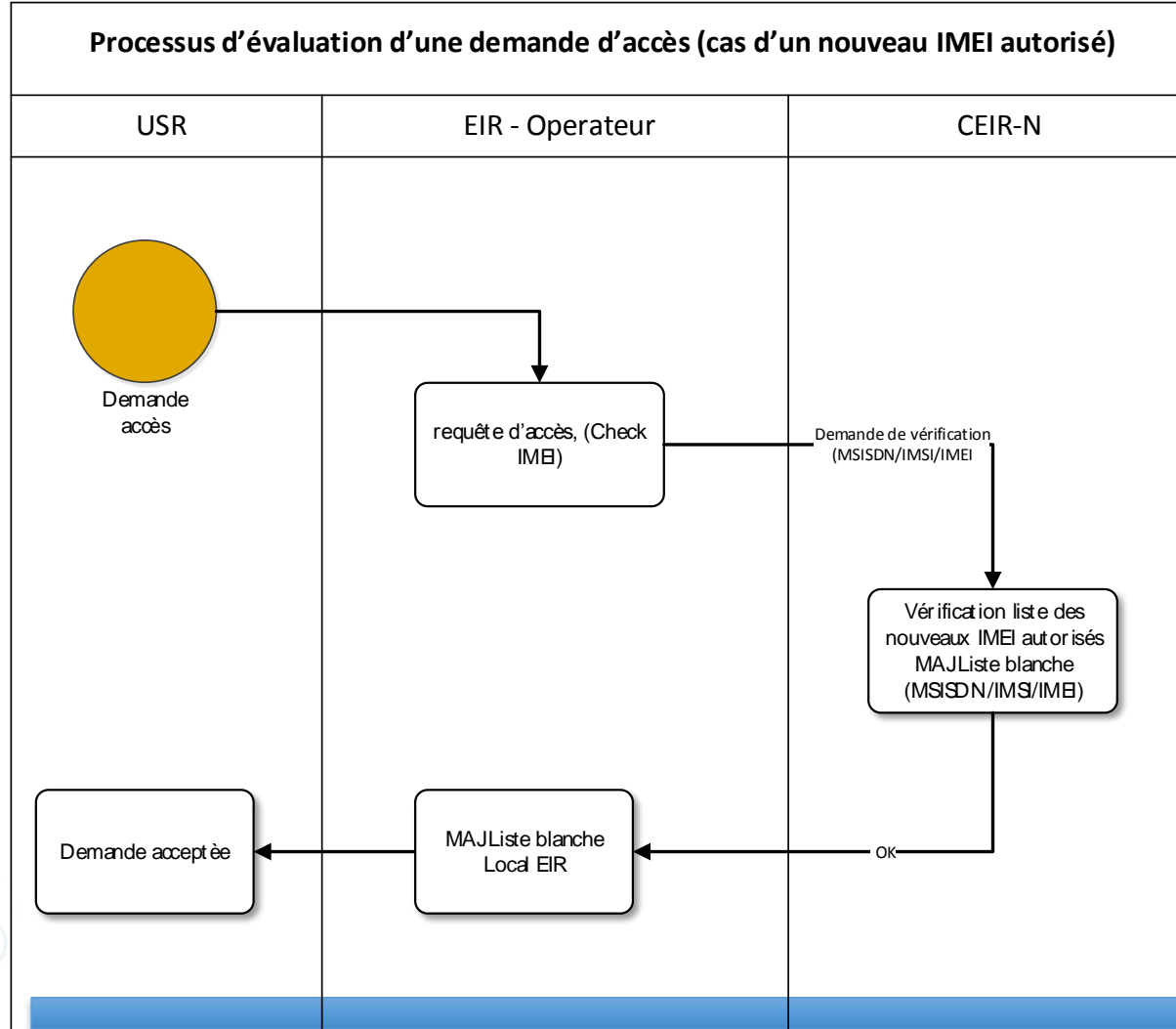
Initial loading

The CEIR-N database must be initially loaded from all the lists (LIMEI-CERT and LIMEI-EIR) of the IMEIs of the mobile terminals which are respectively stored in the databases of CERT and those of the EIRs used by the operators of public mobile networks.
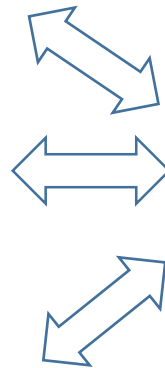
Evaluation of a new authorized terminal

Processus d'évaluation d'une demande d'accès (cas d'un nouveau IMEI autorisé)		
USR	EIR - Operateur	CEIR-N

Demande accès

requête d'accès, (Check IMEI)

Demande de vérification (MSISDN/IMSI/IMEI)

Vérification liste des nouveaux IMEI autorisés MAJ Liste blanche (MSISDN/IMSI/IMEI)

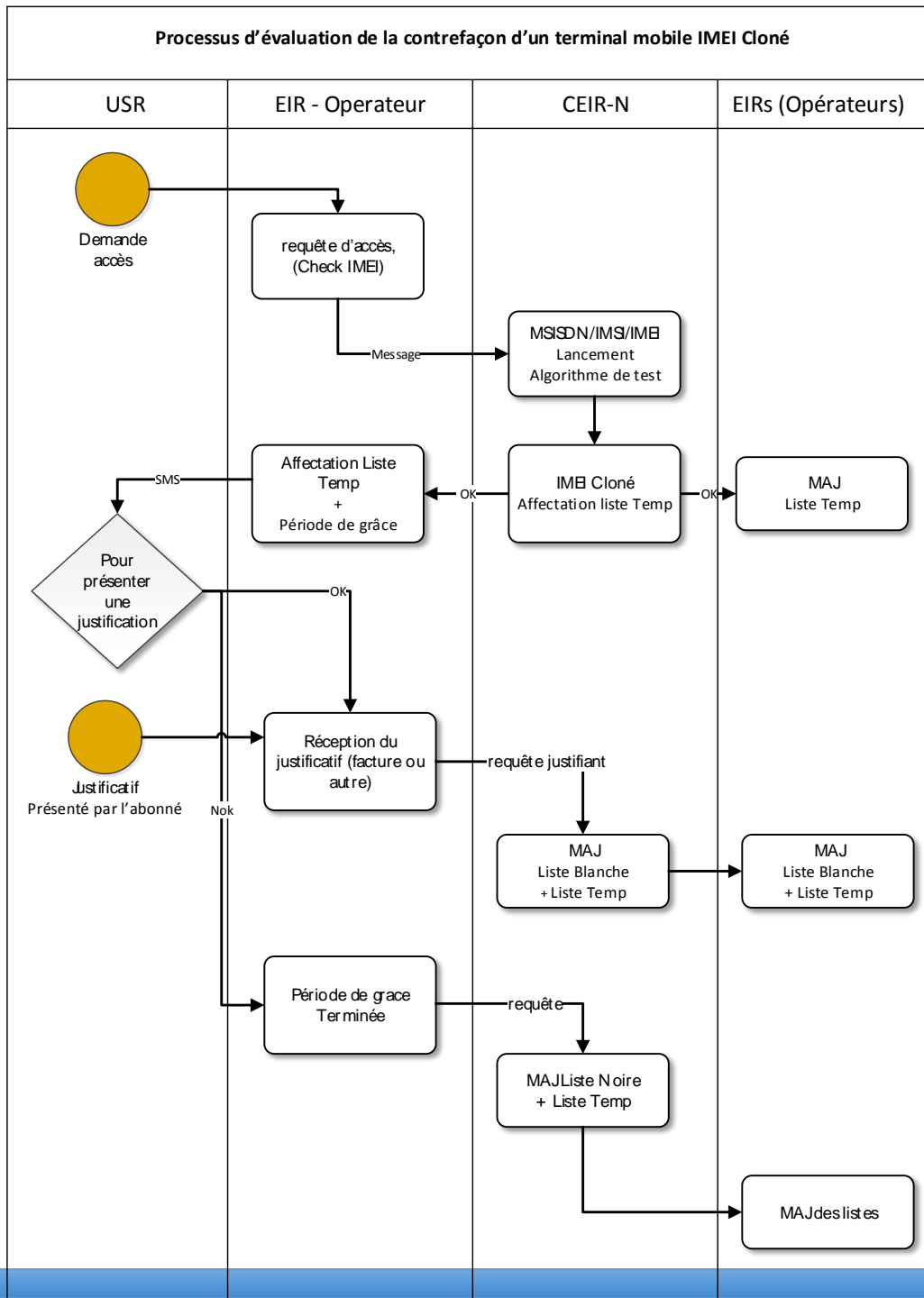Demande acceptèe

MAJ Liste blanche Local EIR

OK

Process

Invalid IMEI case or IMEI = 0

At the moment an operator detects an erroneous IMEI or IMEI = 0,
the subscriber will automatically be rejected from the network.

Process

Counterfeit case of a mobile terminal

Processus d'évaluation de la contrefaçon d'un terminal mobile IMEI Cloné

USR	EIR - Operateur	CEIR-N	EIRs (Opérateurs)

Demande accès

requête d'accès, (Check IMEI)

Message

MSISDN/IMSI/IMEI
Lancement
Algorithme de test

Affectation Liste Temp + Période de grâce — SMS

IMEI Cloné
Affectation liste Temp — OK

MAJ
Liste Temp — OK

Pour présenter une justification

Justificatif
Présenté par l'abonné

Réception du justificatif (facture ou autre) — OK / Nok

requête justifiant

MAJ
Liste Blanche
+ Liste Temp

MAJ
Liste Blanche
+ Liste Temp

Période de grace Terminée

requête

MAJ Liste Noire
+ Liste Temp

MAJ des listes
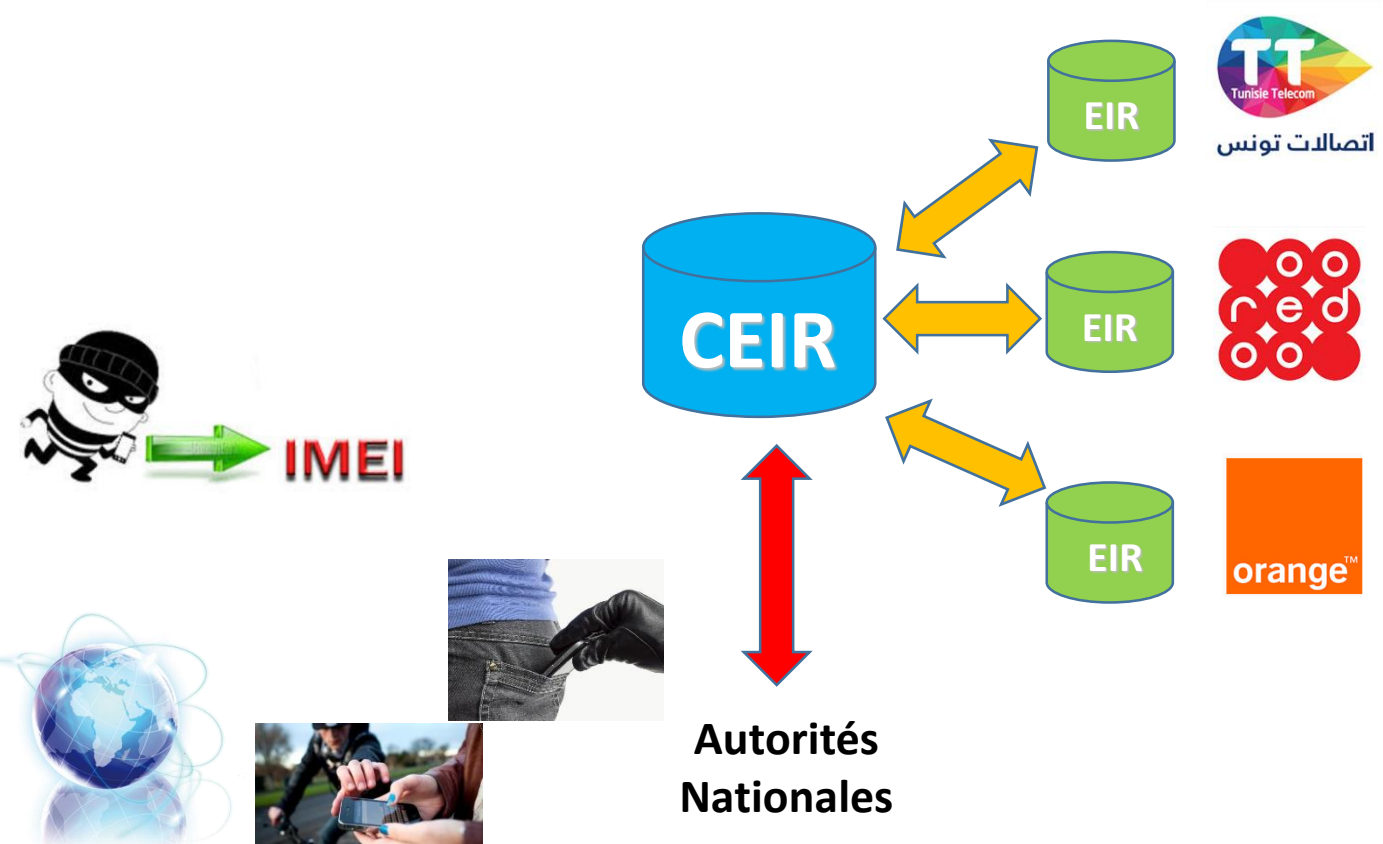
Case of a foreign mobile terminal

- If the subscriber is roaming, he accesses the network,
- If the subscriber wants to use his terminal for a short period in Tunisia with a local SIM, in this case the operators will assign him a "tourist SIM", after presenting the necessary supporting documents. Then, the terminal can access to the network during a grace period T.
- In case of decision to:
  - become resident in Tunisia
  - to exceed the period T
  - to give up his terminal,
⇨ the subscriber is called to register his terminal.
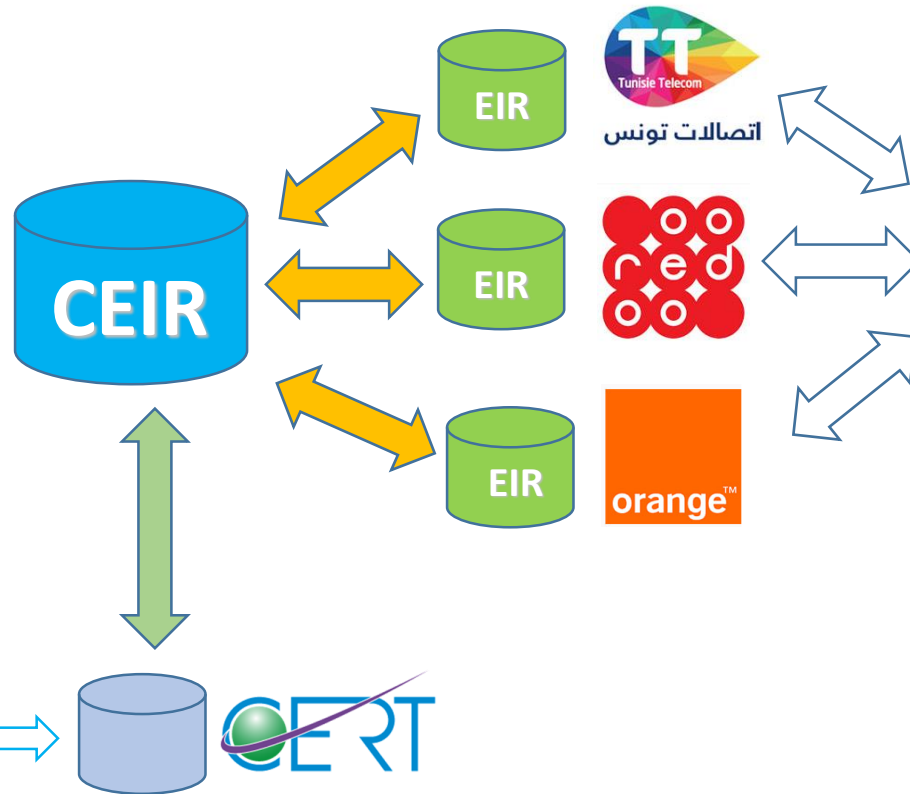
Process

Case of theft or loss of a mobile terminal

Only the national authorities will be able to change the IMEI from the whitelist to the blacklist or vice versa.

Autorités Nationales

Thanks