

Mobile-Communication

“ [!toc] Table of Contents

First, some basic information about threats in the field of mobile communications needs to be explained. This article focuses on how a single cell phone communicates with the mobile network in the form of a cell phone tower (colloquially: antenna mast). The terms IMSI and IMEI (and sometimes TMSI) appear frequently and are also briefly explained here.

Who owns cell phone towers?

Cell phone towers are operated by mobile phone providers. Accordingly, the respective mobile phone providers also control the data traffic passing through these towers. In the image below, the different colors symbolize different providers (in Germany), such as Telekom, Vodafone, O2, etc.

Map symbolically showing how cell phone towers are distributed in a city

IMSI: SIM identifier

Every SIM card has a unique identifier, the International Mobile Subscriber Identity, or IMSI for short. Due to the registration requirement for SIM cards in most European countries, the SIM card is usually uniquely assigned to an identity. The authorities can easily request this information from mobile phone providers and do so very regularly.

Authorities can ask the providers which phone numbers belong to a certain person. This can also work in the other direction, for example asking who the owner of number 0123456789 is. Those inquiries are very cheap for authorities and are regularly used on a massive scale.

IMEI: Device identifier

Mobile phone modems (i.e., the chip in your cell phone that can connect to the mobile network) also have a unique number, the International Mobile Equipment Identity, or IMEI for short. These IMEIs are usually 15 digits long and globally unique. The structure is as follows:

- The first 8 digits are, to put it simply, type-specific. For example, all Google Pixel 7a devices have the following 8 digits: 35917382
- The next 8 digits are serial numbers
- *The last digit is for error correction*

picture of IMEI sets of different models from same and different vendors next to each other.

“ [!technical] How is it ensured that these numbers are unique?

Since many different companies produce such mobile communications modems, it is necessary for them to coordinate with each other. Otherwise, with thousands of modems produced every day, numbers would quickly be assigned multiple times.

This is handled by the **GSMA** (Global System for Mobile Communications Association). The name speaks for itself.

- So if a manufacturer wants to launch a new model, they go to the GSMA and ask for a “number space,” the first 8 digits. They can then name all chips produced for this model with this number space, i.e., assign IMEIs.
- The serial numbers are used to distinguish individual devices of the same model.
- Error correction is a bit of black magic and can really be ignored here.

“ [!detail] EIR: (Equipment Identity Register)

However, the standard also provides for “whitelists.” This would mean that all IMEIs produced are recorded and only those recorded are allowed to participate in the network. This would then be a significant security risk if a cell phone is purchased with traceable payment methods.

Examples of modem manufacturers: Qualcomm, Huawei, ZTE, Sierra Wireless, Netgear, Alcatel, TP-Link

The IMEI therefore makes every mobile device identifiable.

If a device can be used with multiple SIM cards at the same time (regardless of whether these are two physical SIM cards or one e-SIM and one physical SIM card), it also has the corresponding number of IMEIs.

However, it is often quite easy to establish a connection between these two IMEIs:

- The serial numbers are often simply incremented (*except for error correction*)
- If two IMEIs are always in the same place, this can be correlated
- The manufacturers and retailers know the correlation between the two IMEIs
- If an EIR is involved, these two IMEIs are also linked to each other in the EIR. So if one of the two IMEIs is known, the second one can also be found in the EIR.

The IMEIs cannot be changed easily. In many countries, manipulating them is a criminal offense. It also requires special hardware, which is most likely to be obtained from China.

“ [!tip] Tip {static}

There are some [mobile routers](#) that can be flashed with a special operating system named [blue merle](#). Blue Merle can be used to change the routers IMEIs and can also be configured to only use TOR.

Problems when buying cell phones

So if you buy a phone in a store and pay with a card, the store will have a link between your card and the IMEI(s) of your phone. As a result, authorities may be able to trace the IMEIs assigned at the factory to specific devices by querying sellers and device manufacturers.

And if the cell phone was purchased using your own identity, this association also may exist. However, we do not yet know whether and how often authorities query this association.

“ [!abstract] Conclusion: IMEI {static}

- Identifier of a device, not the SIM card
- Globally unique (by factory default)
- Transmitted to mobile network providers when connected to a mobile network (see [Authentication](#))

Authentication

Schematic representation of the authentication process between SIM and cell phone tower

- If the mobile phone detects the signal of a cell phone tower, it tries to “knock” on it with a kind of “Hello” to see if the tower is even reachable and, if so, tells it that it would like to log into the network: "I want to log in!"

- If the radio cell receives this message, it first asks for the identity of the mobile phone to ensure that it has the right to log in: "Who are you?"
 - The mobile phone then sends the IMSI of its SIM card to prove that it has the right to connect. At the same time, it also sends the IMEI of its mobile modem (i.e., of the mobile phone).
 - A Telekom cell phone tower would therefore reject a Vodafone SIM card and tell it that it does not have the right to use the Telekom network.
 - This completes the authentication process and a connection can be established. The purpose of the TMSI is secondary here and has therefore been removed for simplification.
 - According to the standard, such connections can only be established in "encrypted" form.
- You can read why this is in [missing quota](#).

“ [!technical] What is the TMSI?

If a connection were simply established, anyone nearby with the appropriate hardware (e.g., software-defined radios starting at €20) could see which cell phones are currently logged into the network with which SIM cards and how much they are communicating.

To prevent this from happening, the procedure goes one step further: The cell phone tower gives the cell phone a TMSI (Temporary Mobile Subscriber Identifier). From now on, the mobile phone uses this TMSI for identification, but only in this session. If the mobile phone logs out of this tower at some point and logs back in later, the entire procedure starts again and a new TMSI is assigned.

If you are still wondering why the mobile phone needs to identify itself again after the initial authentication: Sent packets always need recipients (and senders), of course. So that your mobile phone can be found again during a connection to a website, for example, in order to present the content to you, "the network" must of course know which device you are.

Both the IMSI and the IMEI are transmitted during authentication with the mobile network. This creates traceable data for mobile phone providers that enable a unique assignment between IMSI and IMEI, i.e., cell phone and SIM card.

Therefore you should be aware of this risk when using a mobile phone that has previously been used with another SIM card, which in turn allows conclusions to be drawn about your own identity. In addition, the mobile phone may also have ended up in a [Geofence warrant](#) with another SIM card.