DFS Professional CDMA Tool FAQ

Powered by Telecom Logic group

DFS CDMA
Professional CDMA Software

Frequently Asked Questions
September, 2013

FAQ CDMA Tool
1. What is ESN?

ESN (Electronic Serial Number) - were created by the U.S. Federal Communications Commission (FCC) to uniquely identify mobile devices. Code 0x80 is reserved from assignment and is used instead as prefix for pseudo-ESNs (pESN). Pseudo-ESNs are not guaranteed to be unique (the MEID is the unique identifier if the phone has a pseudo-ESN).

As ESNs have essentially run out, a new serial number format, MEID, are 56 bits long. The main difference between MEID and IMEI is that the MEID allows hexadecimal digits while IMEI allows only decimal.

2. What is MEID?

MEID (Mobile Equipment Identifier) - is a globally unique number identifying a physical piece of CDMA mobile station equipment. The MEID was created to replace ESNs, the ESN is still a required field in many messages—for compatibility, devices with an MEID can use a pseudo ESN (pESN), which is a manufacturer code of 0x80 (formerly reserved) followed by the least significant 24 bits of the SHA-1 hash of the MEID.

3. Where you can determinate the your phone ESN or MEID?

In most cases label on back side of phone contain information about Model, FFCID, and other info include ESN and MEID. It may be show in decimal (Dec) or hexadecimal (Hex) format:
Sometimes the MEID or ESN printed on the label does not match with MEID or ESN stored in phone. Actual MEID or ESN displayed in Status/Info menu most amounts of phones or can be read from DFS Tool.

4. What is the difference between MEID Dec and MEID Hex?

These are just two ways of representing the same parameter MEID. To convert from Hex to Dec and back from Dec to Hex you can use http://www.meidconverter.com or DFS Tool.

5. How can I get pESN from MEID?

U can calculate pESN from MEID using http://www.meidconverter.com or DFS Tool. Just type your MEID in Dec or Hex format and pESN automatically shows when you complete typing.
6. What is NAM?

NAM (Number Assignment Module) A part of the phone that stores a wireless device's MDN, MIN, PRL, lock code, and other user information. The NAM is programmed by the service provider when a device is activated. These parameters include the PRL, MDN, (MSIN) MIN, MMC, MNC, SID, NID, A-key, Preferred Mode, Hybrid Mode, 3G provision and MIP settings. Depend of carrier some of network parameters may not used. Minimal NAM parameters qty. uses in old 2G CDMA Network, Only MIN and PRL need write to phone to make available voice calls.

7. What is MDN?

MDN (Mobile Directory Number) The actual phone number one would dial to reach a specific mobile phone. Prior to Wireless Number Portability, MDN was the same number as the MIN for many mobile phones. But now that MDN numbers can be ported (moved) to other carriers, MDN and MIN will be different for ported numbers.

8. What is MIN (MSIN)?

MIN (Mobile Identification Number), MSIN (Mobile Subscriber Identification Number) A unique 10-digit number assigned by the wireless service provider (carrier) to each phone it sells or includes in service plans. Unlike an Electronic Serial Number (ESN), a MIN is changeable because wireless phones may change hands or phone owners may move to another coverage region, requiring a different service plan.
9. What is IMSI?

IMSI (International Mobile Subscriber Identity) is a 15 digit length globally-unique code number that identifies a mobile subscriber to the network. The IMSI is linked to your account information with the carrier. IMSI consist of three parts MCC, MNC and MIN (MSIN). A mobile network code (MNC) is used in combination with a mobile country code (MCC) (also known as a "MCC / MNC duple") to uniquely identify a mobile phone operator/carrier using the GSM/LTE, CDMA and some satellite mobile networks.

For example Verizon wireless: MCC = 310, MNC = 00, MIN = 1122334455 than IMSI is MCC+MNC+MIN = 310001122334455
9. What is SID?

A System Identification Number (SID) is broadcast by one or more Base Stations to identify a cellular network in a certain area (usually contiguous). It is globally unique within CDMA networks. When the phone is turned on, it listens for a signal. If it receives a signal, it looks at the SID (being carried by the signal), and compares it with the one that is stored in the phone. Originally, in analog systems, the mobile would simply turn on the roaming indicator if the SID was not the single value stored in the phone. However, with CDMA systems the Preferred Roaming List (PRL) is responsible for determining which areas a mobile can roam into. Base stations may also broadcast an MCC and MNC which can also be used by the PRL.

10. What is PRL?

PRL (Preferred Roaming List). The PRL is a list of information that resides in the memory of some kinds of digital phones. It lists the radio frequencies the phone can use in various geographic areas. The part of the list for each area is ordered by the bands the phone should try to use first. Therefore it’s a kind of priority list for which towers the phone should use. The PRL helps determine which home-network towers to use, and also which towers belonging to other networks to use in roaming situations (areas where the home network has no coverage.) When roaming, the PRL may instruct the phone to use the network with the best roaming rate for the carrier, rather than the one with the strongest signal at the moment. Since a PRL tells the phone "where" to search for a signal, as carrier networks change over time, an updated PRL may be required for a phone to "see" all of the coverage that it should, both with the home network and for roaming.

You can check your PRL ID on Status/Info menu of your phone, or can read PRL with DFS Tool and see PRL ID
11. What is OTAP?

OTA (Over-the-air programming) refers to various methods of distributing new software updates or configuration settings to devices like cellphones. In the mobile content world these include over-the-air service provisioning (OTASP), over-the-air provisioning (OTAP) or over-the-air parameter administration (OTAPA), or provisioning handsets with the necessary settings with which to access services such as WAP or MMS. Some phones with this capability are labeled as being "OTA capable".

Depending on implementation, OTA software delivery can be initiated upon action, such as a call to the provider's customer support system or other dialable service, or can be performed automatically. Typically it is done via the former method to avoid service disruption at an inconvenient time, but this requires subscribers to manually call the provider.

*Verizon Wireless* in the U.S. provides a number of OTA functions to its subscribers via the *228* service code. *Cricket* in the U.S. provides a number of OTA functions to its subscribers via the *228* service code. *MetroPCS* in the U.S. provides a number of OTA functions to its subscribers via the *22804* service code.

12. What is Diagnostic (DIAG) mode?

Diagnostic (DIAG) mode is the mode in which to put the phone via different ways (usually by dialing special DIAG codes) to make available reading and/or writing NAM parameters responsible for the correct operation of the phone with own ESN in a particular operator's network.

You can find DIAG codes for most phones model in Comment field of DFS Tool.
13. What is Emergency (Download) mode?

Emergency also Download mode, it is special phone mode that make available upgrade or replace firmware with DFS Tool or special vendor PST.

14. What is a Diagnostic driver?

This is a driver required by the operating system to recognize the connected equipment is in diagnostic mode. Each manufacturer supplies the drivers for their devices. **Drivers** are different by type (Win8, Win7, Win XP) and 32/64 bit operating system. May be as installation software package or in the form of files requiring manual setup. The most uses drivers you can find on **DFS Tool** download page [http://cdmatool.com/download](http://cdmatool.com/download)

15. Unlock, what does it mean?

Many mobile carriers provides **CDMA** or **GSM** phones to their subscribers as a way of ensuring the phones are not usable on rival networks, employ special software "locks" that prevent use of the phone on other networks, and you must unlock the phone if you want to use it with another provider.

There are different types of software “locks”, such as:

**MIN Lock** – in this case phone accept to write and store only MIN from carrier specified range.

**SPC (Security Provider Code)** – In this case phone not accept writing and store any NAM parameters while user not sending to phone a known 6 digit code. When talking about Unlock to remove network restrictions for **CDMA** phones, most means reset SPC code to **000000**.

**SIM Lock** - A **SIM lock, simlock, network lock or subsidy lock** is a capability built into mobile phones by mobile phone manufacturers. Network providers use this capability to restrict the use of these phones to specific countries and network providers. Generally, phones can be locked to accept only **SIM/RUIM** cards with certain **International Mobile Subscriber Identities (IMSI)**; **IMSI** may be restricted by:

- Mobile country code (**MCC**; e.g., will only work with SIM issued in one country)
- Mobile network code (**MNC**; e.g., Sprint, Boost, Virgin Mobile, etc.)
- Mobile subscriber identification number (**MSIN**; i.e., only one SIM/RUIM can be used with the phone)
User Lock – in this case it means possibility of regarding 4-digit user password. Also present special unlock types for make possible repair extra security parameters like MEID, ESN, A-Key, 3G provision keys. This unlock types depend of many factors like phone vendor, phone model, firmware version and others.

16. Activation what does it mean?

Currently, the Activation term means of many concepts that can easily confuse the newbe users. Activation relating cellular operators:

Activation screen can be seen at the terminals made by one of the mobile operators (Verizon, Sprint, MetroPCS, etc.) The serial numbers of these terminals are included in the database of the operator. In this case, the user dialing OTAP (*228. *22804 and so on.) Following the instructions of auto-informer and activates the terminal to a new or existing phone number of the operator.

It is also understood by the term activation to add the base cellular operator serial number (ESN) of the machine, and the association with him the phone number (MIN, MDN). You can do this in several ways:
1. Through technical support operator or through a dealer network.
2. Self-subscriber through online control panel (if applicable).

MetroPCS [http://www.metropcs.com/metro/activation/activation.jsp](http://www.metropcs.com/metro/activation/activation.jsp)

Some operators do not allow you to activate third-party terminals.
**Activation** related to the terminals **Apple**:

For **Apple** terminals there are two types of activation. The first passes through **iTunes** or direct access to the Internet via **Wi-Fi**.

The second type of activation of the terminal **Apple** requires proper programming operator network configuration. This can be achieved in two ways. Via **OTA** service where it is possible to program the terminal or by using **DFS Tool**.

Intellectual property of DFS Team. 2003-2013
[http://www.cdmatool.com](http://www.cdmatool.com)
iPhone Activation of the service [http://www.cdmatoool.com](http://www.cdmatoool.com) involves adding **iPhone MEID** to an users with [www.cdmatoool.com](http://www.cdmatoool.com) account, which allows the reprogram the **iPhone** in the future indefinitely. Activation fee is $50.

### 17. What is Vocoder?

**Short for voice encoder.** A device that encodes and decodes the sound of human voice into/from digital format for transmission. Different **vocoder** types may produce digital data of different bitrates (amount of data per second).
Higher bitrates may indicate better voice quality, although more efficient vocoders can achieve high voice quality with lower bitrates.

18 What is A-key?

Authentication key (A-key) – A 64-bit primary secret key known only to the phone and Authentication Center. In the case of RUIM equipped mobiles, the A-key is stored on the RUIM; otherwise, it is stored in semi-permanent memory on the phone. The A-key is never shared with roaming partners. However, it is used to generate a secondary key known as SSD that may be shared with a roaming partner to enable local authentication in the visited network.

19. What is SSD_A, SSD_B?

Shared Secret Data (SSD) – A 128-bit secondary secret key that is calculated using the CAVE algorithm during an SSD Update procedure. During this procedure both phone and the Authentication Center in the user’s home network separately calculate SSD. It is this SSD, not the A-key that is used during authentication. SSD may or may not be shared between home and roaming partner networks to enable local authentication. SSD consists of two 64-bit keys: SSD_A, which is used during authentication to calculate authentication signatures, and SSD_B, which is used in the generation of session keys for encryption and voice privacy.

20. What is Voice Privacy?

When you enable Voice Privacy, your phone starts encrypting your calls so nobody can eavesdrop on them. By encrypting your phone calls between your phone and the base station, you add an extra layer of protection on your calls just in case someone wants to try to listen in. For this feature to work, your cellular service provider must support it, otherwise enabling it on your phone is useless.

21. What is RUIM?

A removable user identity module (RUIM or R-UIM) card is an identification chip for cell phones that work on Code Division Multiple Access (CDMA) networks. A RUIM card stores a user's personal information, such as his or her name and account number, phone number, address book, text messages, and other settings. These cards can be swapped between compatible phones, so the user's information and settings are easily transferred. In many cases, a RUIM card can also be used in a phone designed to work on the Global System for Mobile Communication (GSM) network.

22. What mean phone operate in RUIM mode?

Many telephones and modems manufactured recently support both modes of operation. The first mode - provides a works with RUIM cards. Second - NV mode operation with the settings stored in the internal memory of the phone. Correct writing of parameters in the internal phone memory, when it is in RUIM mode is not possible. Check in what mode the terminal, and to implement switching between modes by using the DFS tool.
**CDMA phones** technically can be unlocked but not in the same sense that people think about **GSM** and iDEN unlocking. Since **CDMA** phones do not use a **SIM** card, they are sort of "hardwired" to the provider that sells them. Therefore, they can only be unlocked by the provider with a special code that they absolutely will not give out over the phone. This contrasts how you might call Cingular and have them give you an unlock code so you can travel overseas and use your **GSM** phone with a foreign **SIM** card. **GSM** phones can usually be unlocked remotely, but **CDMA** phones require a bit of 'reprogramming' to unlock, and it's not as simple as calling your provider and getting a code over the phone.

Generally, **CDMA** phones are **NOT** considered unlockable because it is usually impractical to do so. Sprint, my provider, will not under any circumstances activate a non-Sprint phone, so an unlocked **CDMA** phone would be useless to you if you use Sprint. Even if you get an unlocked **CDMA** phone and by some chance are able to have it activated with your provider, many of the features will not work correctly unless someone with quite a bit of technical knowledge reprograms the phone to your provider's specifications.

So, you can see where this is a very confusing subject. Even if you can unlock your **CDMA** phone, who is going to activate it for you? I suggest you call your **CDMA** provider, whether it's Sprint, Verizon, or whoever, and ask them if they will activate an unlocked Treo. Don't be surprised if they either act like they don't know what you're talking about, or even laugh at you for asking. You may have to ask for a level-2 tech person before you even get an acknowledgement that **CDMA** unlocking is possible. Your best chance is with a prepaid service, as they generally do not care where the phone comes from as long as you are buying their minutes, but I would still suggest calling them and asking before you spend the money on a phone.