

Over-The-Air Provisioning in CDMA

by

Rohini P.P.
Gemplus Technologies

October 2004

Abstract: *This paper gives an introduction to Over-the-Air Provisioning technology in CDMA from RUIIM point of view. It covers downloadable features and security aspects in Over-the-Air Provisioning.*

TABLE OF CONTENTS

1. INTRODUCTION	3
WHY "OVER-THE-AIR" PROVISIONING?	3
2. OVER-THE-AIR PROVISIONING	3
DOWNLOADABLE FEATURES IN OVER-THE-AIR PROVISIONING TECHNOLOGY	3
<i>a. Number Assignment Module (NAM) operational parameters</i>	4
<i>b. A-Key</i>	4
<i>c. System Selection For Preferred Roaming (SSPR)</i>	5
<i>d. Preferred User Zone List (PUZL)</i>	5
<i>e. 3G Packet Data (3GPD) operational parameters</i>	5
3. SECURITY	5
<i>a. Service Programming Lock (SPL)</i>	5
<i>b. Subscriber Parameter Administration Security Mechanism (SPASM)</i>	5
<i>c. Secure Mode</i>	5
4. GEMPLUS AND CDMA OVER-THE-AIR PROVISIONING	6
5. CONCLUSION	6
REFERENCES	7
GLOSSARY	7

1. INTRODUCTION

CDMA is a digital wireless technology that offers a number of advantages over other mobile communication technologies. Frequency reuse, power control, enhanced voice privacy and soft hand-off are some of them. Smart Cards, known as R-UIM (Removable User Identity Module), are widely used in CDMA phones these days. This article gives an introduction to Over-the-Air provisioning technology in CDMA from the RUIIM point of view.

CDMA: Code Division Multiple Access

CDMA is one of the multiple access systems that allows many users to occupy the same time and frequency allocations. Users are distinguished by unique codes. To achieve this, CDMA uses Spread Spectrum technology in which a signal occupies wider bandwidth than needed. By using the code, bandwidth spreading is performed before transmission. The same code is used for demodulation at the receiving side.

Why "Over-the-Air" Provisioning?

Considering the advantages CDMA offers, suppose an operator sets up a CDMA network. The operator is looking at enhancing its customer base i.e. increasing the number of subscriptions on the network. However, for every new subscription, the process of activation on a CDMA network is complicated, time-consuming and expensive. Also, making changes to the existing subscription (such as changing the phone number) is operationally difficult since the customer has to physically take the phone back to the operator or the retailer. If such changes could be done "Over-the-Air", the process is simplified and made efficient to a large extent. It is in this context that OTAPA (Over-the-Air Parameter Administration)/OTASP (Over-the-Air Service Provisioning) comes into the picture.

Some of the advantages of Over-the-Air provisioning are:

- Increased customer satisfaction
- Point-of-sale retailers do not need to train staff to undertake activation procedures
- Operators have number of benefits such as avoiding pre-programming of handsets, reducing the number of resources allocated to service provisioning etc.

2. OVER-THE-AIR PROVISIONING

Over-the-Air provisioning can be initiated in two ways: by the network or by the user.

Network initiated session (OTAPA): OTAPA session starts when the network sends OTAPA request command with START/STOP bit equal to one. This is not allowed if the user-initiated session is in progress.

User initiated session (OTASP): OTASP session starts when user manually enters the activation code for the selected system.

Downloadable features in Over-the-Air Provisioning technology

Using this Over-the-Air technology, following features can be downloaded to the RUIIM:

- a. Number Assignment Module (NAM) operational parameters
- b. A-Key
- c. System Selection for Preferred Roaming (SSPR)
- d. Preferred User Zone List (PUZL)
- e. 3G Packet Data (3GPD) operational parameters

a. Number Assignment Module (NAM) operational parameters

Mobile Directory Number, Access Overload Class, IMSI value and SID NID pair (System Identification Number, Network Identification Number) are some of the values that come under this category. Activating a new service or making changes to the existing service is made through these parameters. Download Request and Configuration Request are the commands used to achieve this.

b. A-Key

The A-Key, which is used in CDMA Authentication process, is re-programmable. A-Keys can be programmed using any of the following ways:

1. At the factory
2. At the point-of-sale
3. Subscribers via telephone
4. Over-the-Air provisioning

Security of the A-Key is critical in a CDMA system. Over-the-Air provisioning uses Diffie-Hellman algorithm, making it the best choice for A-Key programming from the alternatives mentioned above. Diffie-Hellman algorithm is used for secure key exchange between two entities so that a third party cannot deduce the value in the process of exchange.

How does the Diffie-Hellman algorithm work? : To understand this algorithm consider the following example:

Let P (Modulus) be a large prime number and G (Generator) an integer base less than P. P and G are known to two entities A and B. x and y are two other numbers which are private and known only to A and B respectively.

Let $\alpha = [G^x] \text{ mod } P$ and $\beta = [G^y] \text{ mod } P$

Now, A and B exchange the values α and β . After getting the other entity's values, A calculates

$\alpha' = [\beta^x] \text{ mod } P$ and, B calculates $\beta' = [\alpha^y] \text{ mod } P$. It can be mathematically proved that $\alpha' = \beta'$

Thus it can be seen that even though A and B started with different private values x and y, through the Diffie-Hellman algorithm they have derived a common value without exposing their private values. (Please note that the above example is just an illustration and the actual implementation requires certain conditions to be met while selecting the numbers P, G, x and y.) It is this methodology that is adopted in a CDMA network while programming A-key Over-the-Air.

How A Key is programmed through Over-the-Air? : There are two commands MSKey Request and Key Generation Request, which are used in Programming A Key.

MSKey Request - In this step the numbers P and G are sent to the RUIM from the network. The ME also generates a random number and sends it to the RUIM along with P and G. The RUIM may use this random number for generating its private number x. It then calculates $\alpha = [G^x] \text{ mod } P$ and stores the result.

Key Generation Request - The network sends $\beta = [G^y] \text{ mod } P$, where y is the network's private number, to the RUIM. In response to this, RUIM sends α to network. Now, the R-UIIM calculates $\alpha' = [\beta^x] \text{ mod } P$ and the network calculates $\beta' = [\alpha^y] \text{ mod } P$ respectively. As described above, $\alpha' = \beta'$ and a subset of this common value is the A-key.

c. System Selection For Preferred Roaming (SSPR)

Preferred Roaming List (PRL) contains information that ME uses for system selection and acquisition. PRL File can be programmed Over-the-Air, which makes the process efficient and convenient for both the mobile subscriber as well as for the operator. SSPR Download Request and SSPR Configuration Request are the commands used in this case.

d. Preferred User Zone List (PUZL)

Preferred User Zone List provides the priority and characteristics of the user zones to which the mobile station is subscribed. After the mobile station completes system acquisition using PRL, PUZL is used to select the most preferred user zone in that system. User zone insert, User zone update, User zone delete etc. can be performed Over-the-Air. PUZL Download Request and PUZL Configuration Request are the commands applicable.

e. 3G Packet Data (3GPD) operational parameters

3G Packet Data (3GPD) operational parameters can also be programmed Over-the-Air. Various parameters related to Simple IP and Mobile IP come under this category. The commands used are 3GPD Download Request and 3GPD Configuration Request. For details on how to download the above-mentioned parameters, please refer 3GPP2 standards.

3. SECURITY

As can be seen from the discussions above, in OTAPA/OTASP all the provisioning is performed over the air. Therefore it is important that security features are robust. Following are the main security features associated with Over-the-Air provisioning:

a. Service Programming Lock (SPL)

The Service Programming Lock (SPL) protects the mobile station programming module that can be assigned values using Over-the-Air provisioning. The Service Programming Code (SPC) is stored in EF spc. If the SPC value is not zero, before programming, a correct value of SPC needs to be presented. Otherwise, for any programming command, RUIM will return the status 'Mobile Station Locked'. Verification of SPC is performed by use of the 'Validate Request' message.

b. Subscriber Parameter Administration Security Mechanism (SPASM)

Subscriber Parameter Administration Security Mechanism (SPASM) Protection is based on signature verification. There is no SPASM protection for user-initiated session; it is applicable only for session started by a network. Once RUIM receives the message 'OTAPA Request', it calculates a signature based on some parameters that are known to both RUIM and the network and stores this value. RUIM validates SPASM by comparing the signature received in the 'Validate Request' message from the network to its own computed value.

c. Secure Mode

Secure Mode is a mechanism for improving the security of a programming session. Once the Secure Mode is active, the data fields of all provisioning messages exchanged between RUIM and network will be encrypted.

4. GEMPLUS AND CDMA OVER-THE-AIR PROVISIONING

Gemplus, the innovative pioneer in Smart Cards industry, has many CDMA products including Javacards. Further, Gemplus is an active member of the CDMA standardization committee. In 2001, Gemplus released *GemXplore World* that supports OTAPA/OTASP features along with CDMA ANSI 41 commands.

5. CONCLUSION

CDMA has proved to be a promising technology for 3G networks. As described in this paper, application of Over-the-Air provisioning to CDMA brings in a number of advantages such as flexibility, improved efficiency, increased customer satisfaction and eventually enhanced revenue generation for the operator. Therefore, the synthesis of Over-the-Air provisioning technology with CDMA is expected to be one of the technologies for the future. One of the critical components to make this process work is the RUIIM.

REFERENCES

1. 3GPP2 C.S0023-B Version 1.0, *Removable User Identity Module for Spread Spectrum Systems*.
2. 3GPP2 C.S0016-B Version 2.0, *Over-the-Air Service Provisioning Of Mobile Stations in Spread Spectrum Standards*.
3. *CDMA 1XRTT Security Overview* by Christopher Wingert and Mullaguru Naidu, Qualcomm Inc. August 2002

GLOSSARY

2G	2nd Generation
3GPD	3G packet data
ANSI	American National Standards Institute
CDMA	Code Division Multiple Access
IMSI	International Mobile Subscriber Identity
ME	Mobile Equipment
NAM	Number Assignment Module
NID	Network Identification Number
OTAPA	Over The Air Parameter Administration
OTASP	Over The Air Service Provisioning
PRL	Preferred Roaming List
PUZL	Preferred User Zone List
R-UIM	Removable User Identity Module
SID	System Identification Number
SPASM	Subscriber Parameter Administration Security Mechanism
SPC	Service Programming Code