

1 3GPP2 S.R0073
2 Version 1.0
3 Version Date: 11 July 2002
4
5
6
7
8
9



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

10 *Internet Over-the-Air Handset* 11 *Configuration Management (IOTA)*

12 13 *Stage 1*

14 15 16 17 18 19 20 21 22 23 24 25 **COPYRIGHT NOTICE**

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

26
27

1 **EDITOR**
2 Mark A. Lipford, Sprint PCS mlipfo01@sprintspectrum.com +1 913.890.4248

3
4 **REVISION HISTORY**

5

REVISION HISTORY		
Revision number	Content changes.	Date
1.0	Initial publication	July 11, 2002

6

Table of Contents

1		
2		
3	Table of Contents	1
4	List of Tables	2
5	List of Figures	3
6	1. INTRODUCTION	3
7	2. REFERENCES	3
8	3. DEFINITIONS AND ABBREVIATIONS	4
9	4. GENERAL FEATURE DESCRIPTION	5
10	5. Requirements	7
11	6 Applicability to Telecommunications Services	10
12	6.1 Normal Procedures with Successful Outcome	10
13	6.2 Authorization	10
14	6.3 De-Authorization	10
15	6.4 Registration	10
16	6.5 De-Registration	10
17	6.6 Activation	10
18	6.7 De-Activation	10
19	6.8 Invocation	10
20	6.9 Normal Operation with Successful Outcome	11
21	7 Exception Procedures or Unsuccessful Outcome	11
22	7.1 Registration	11
23	7.2 De-Registration	11
24	7.3 Activation	11
25	7.4 De-Activation	12
26	7.5 Invocation	12
27	7.6 Exception While Roaming	12
28	7.7 Exception During Intersystem Hand-off	12
29	8 Alternative Procedures	12
30	9 Interaction With Other Services	12
31	9.1 Standard Voice Services	12
32		
33		

1
2
3

List of Tables

List of Figures

1
2
3
4

1. INTRODUCTION

This document specifies the requirements for and operation of Internet based Over-the-Air Handset Configuration Management (IOTA HCM) from the perspective of the users and system operators.

The objective of this document is to define the requirements of this feature for incorporation into the operations of cdma2000 based wireless telecommunications systems.

2. REFERENCES

The document references which are applicable to this specification include the following normative and informative references:

- ?? TIA/EIA-95, Mobile Station - Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System. Published in July 1993.
- ?? TIA/EIA-95-A, Mobile Station - Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System. Published in May 1995.
- ?? TIA/EIA-95-B, Mobile Station - Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System. Published in December 1998.
- ?? C.S0015-0, Short Message Service (SMS). Published in December 1999.
- ?? C.S0016-A, Over-the-Air Parameter Administration of Mobile Systems in Spread Spectrum Systems.
- ?? IS-707, (14.4 kbps) Data Service Options for Wideband Spread Spectrum Systems. Published in February 1998.
- ?? C.S0017-0, (14.4 kbps) Data Service Options for Spread Spectrum Systems- STU III Transparent + Non-Transparent. Published December 1999
- ?? N.S0011, OTASP and OTAPA Enhancements to TIA/EIA-41.
- ?? C.S0023, Removable User Interface Module, published June 2001
- ?? P.S0001-0, cdma2000 Wireless IP Network Standard, published June 2000.
- ?? C.S0001, Introduction to cdma2000 for Spread Spectrum Standards. Published July 2001
- ?? C.S0002, Physical Layer for cdma2000 for Spread Spectrum Standards. Published July 2001

- 1 ?? C.S0003, Medium Access Control Layer (MAC) for cdma2000 for Spread
2 Spectrum Standards. Published July 2001
- 3 ?? C.S0004, Link Access Control Layer (LAC) for cdma2000 for Spread Spectrum
4 Standards. Published July 2001
- 5 ?? C.S0005, Upper Layer Signaling for cdma2000 for Spread Spectrum Standards.
6 Published July 2001
- 7 ?? C.S0006, Analog Signaling for cdma2000 for Spread Spectrum Standards.
8 Published July 2001
9

10 **3. DEFINITIONS AND ABBREVIATIONS**

11 The terms and abbreviations, which are used within this specification are:

Abbreviations

CDMA	Code Division Multiple Access
FA	Foreign Agent
HA	Home Agent
HCM	Handset Configuration Management
HLR	Home Location Register
IOTA HCM	IP-based Over-the-Air Handset Configuration Management
IWF	Interworking Function
MTAS	Mobile Terminal Authorization System
NAM	Number Assignment Module
OTAMD	Over-the-Air Mobile Diagnostics
OTAPA	Over-that-Air Parameter Administration
OTASD	Over-the-Air Software Download
OTASP	Over-the-Air Service Provisioning
PCF	Packet Control Function
PDSN	Packet Data Serving Node
NAI	Network Address Identifier
MN-FA	Mobile Node to Foreign Agent security key
MN-HA	Mobile Node to Home Agent security key
IS-2000	The cdma2000 Specifications C.S0001 – C.S0006
MS	Mobile Station

1 In summary, the functionality currently planned for support by the IOTA Handset
2 Configuration Management services include the following:

3 ?? OTASP

4 ~~///~~ Subscriber initiated initial programming of Number Assignment Modules
5 (NAMs), data options, operating parameters, service provider specific or
6 manufacturer specific parameters (e.g., server IP address, lock code,
7 indicators, menu options, NAI, password, primary/secondary HA, etc.).

8 ~~///~~ Generation and communication of Authentication Key (A-key)

9 ~~///~~ Programming of preferred roaming lists.

10 ?? OTAPA

11 ~~///~~ Network initiated update, possibly with user approval, of individual
12 Number Assignment Modules (NAMs), data options, operating
13 parameters, and service provider specific or manufacturer specific
14 parameters (e.g., server IP address, lock code, indicators, menu options,
15 etc.).

16 ~~///~~ Update of preferred roaming lists.

17 ~~///~~ Generation and communication of Authentication Key (A-key)

18 ~~///~~ 3G Root Key Support

19 ~~///~~ Addition and update of parameters for future services.

20 ~~///~~ Handset must be provisioned in order for OTAPA to be used.

21 ?? OTASD:

22 ?? In order to address customer demands for additional features and to
23 correct software problems in the field, the carriers desire over-the-air
24 support for software and firmware upgrades.

25 ?? OTAMD:

26 ?? In order to facilitate maintenance support for an installed base of mobile
27 stations, OTAMD (over-the-air mobile diagnostics) support is also
28 desired.

29 One (1) viable means, which is of interest to the carriers for providing the desired
30 capabilities, is proposed by this document as indicated below:

31 ?? Implement an IP-based server (i.e. provisioning sever) functionality for all
32 features and applications. The use of IP, provides maximum flexibility for
33 application developers and customer support providers.

34 ?? Leverage the roll out of C.S0017-0 circuit switched data, P.S0001-0 cdma2000
35 packet data, and C.S0015-0, SMS equipment, which many carriers are in the
36 process of deploying, as the transport mechanisms for the air interface.
37 Subsequent to the initial release and pending the availability of packet data
38 support, this platform could be migrated to packet-based transports as well.

5. Requirements

IP-Based OTA Handset Configuration Management services SHALL be able to co-exist and be independent of OTASP.

The IP-based OTA Handset Configuration Management services SHALL support, at a minimum, the following applications:

~~OTASP~~ OTASP

~~OTAPA~~ OTAPA

~~OTASD~~ OTASD

~~OTAMD~~ OTAMD

In addition, the following objectives are intended to be met:

?? Substantially simplify the handset programming process for both the user and the wireless service provider.

?? Increase the speed and efficiency of mobile station parameters programming including reduction in the potential for handset programming errors.

?? Support seamless and semi-automatic update of MS parameters to improve existing services and add support for future services.

?? Support an interactive customer care solution based on a wireless voice and/or data environment.

?? Increase the flexibility and reduce the complexity associated with handset programming and software upgrades.

?? Enhance customer satisfaction by maintaining handset parameters and operations with only minor impacts to the user (i.e., no trip to a dealer or service depot).

?? Protect and safeguard user information.

?? Support capability for different activation modes to benefit various sales channels.

?? Base the implementation on an industry standard platform (IP-based server) for maximum flexibility and minimum restriction and maintenance concerns.

?? Simultaneous voice and data is strongly desired. This allows the customer care representative to communicate with the user during IOTA operations.

The IOTA Handset Configuration Management system SHALL meet the following requirements:

- 1) PROVISIONING SERVER: Overall control of the IOTA Handset Configuration Management system and all programmed/program data SHALL be maintained on a Provisioning Server. This server SHALL be IP-based.

- 1 2) The Provisioning Server SHALL have an interface to the carrier's Mobile
2 Terminal Authorizing System (MTAS) and billing system. This interface
3 serves to synchronize the Provisioning Server to the information in the MTAS
4 and account records. The specific requirements of this interface are vendor
5 specific and not the subject of this system plan. The Provisioning Server
6 SHALL be capable of receiving dynamic updates from the MTAS.
- 7 3) For OTASP and OTAPA functions, this server SHALL be similar in
8 functionality to the OTAF (over-the-air function) specified in IS-725-A and
9 referenced in IS-683-B. The signaling format should be synchronized with
10 C.S0016-A or the latest release whenever applicable.
- 11 4) COMMUNICATION WITH THE MOBILE STATION: Communication
12 with the MS SHALL meet the following requirements:
- 13 ✍ Programming operations SHALL use any IP-based data connection
14 supported by an air interface. For example in IS-2000 based systems, the
15 implementation SHALL support circuit and/or packet data transport
16 services including one (1) or more of the following: IS-C.S0017-0,
17 P.S0001-0, and Quick Net Connect (QNC).
- 18 ✍ This system SHALL also include a capability for network directed
19 programming operations.
- 20 5) INTERWORKING FUNCTION (IWF): The IWF connects the MS to the
21 Provisioning Server via an IP connection.
- 22
- 23 6) IOTA Handset Configuration Management procedures SHALL be able to read
24 and update all applicable handset parameters. The list of parameters capable
25 of being updated SHALL include the items listed herein but MAY also be
26 expanded by future releases of the IOTA Handset Configuration Management
27 standard or by vendor/carrier specific technical specifications and purchase
28 agreements.
- 29 7) IOTA Handset Configuration Management services from the mobile station's
30 home carrier SHALL be capable of being supported when the MS is operating
31 on his home carrier's system or roaming on an alternate serving system which
32 also supports this IOTA standard, with the exception that OTASP services are
33 supported only on the home carrier's system.
- 34 8) Security and integrity of NAM parameters and the NAI Profile SHALL be
35 preserved through the use of a strong Subscriber Parameter Administration
36 Security Mechanism (SPASM). The SPASM SHALL prevent unauthorized
37 network-initiated over-the-air programming from taking place.

- 1 9) The SPASM SHALL distinguish each NAM in a MS having multiple NAMs.
2 In other words, each NAM SHALL be secured separately.
- 3 10) The following data security facilities SHALL also be supported:
- 4 A means for the provisioning server to authenticate the mobile station.
5 A means for the mobile to authenticate the provisioning server.
6 A means for the serving system to authenticate the mobile station such that
7 its security with its home system is not compromised.
8 The security algorithms chosen should be ones, which have been subjected
9 to open review. Public security algorithms, which have been accepted by
10 a large community, have less chance for security holes than private
11 security algorithms due to the rigors of creating public security algorithms.
- 12 11) The security framework selected SHALL be flexible so that one (1)
13 mechanism can be exchanged for another if the target environment, threat
14 model, or the state of technology changes. The ability to exchange one (1)
15 mechanism for another SHALL not itself compromise security.
- 16 12) Security and integrity of air interface communications MAY be preserved by
17 encrypting sensitive data.
- 18 13) Deployment of IOTA SHALL NOT have any impact on existing
19 authentication centers as defined by TIA/EIA-41.
- 20 14) OTAPA MAY be performed by the home carrier without user intervention or
21 knowledge.
- 22 15) The IOTA Handset Configuration Management system SHALL provide
23 support for initiation of any IOTA Handset Configuration Management
24 function either by the MS or the Provisioning Server. However, this
25 capability MAY be limited by the service provider via appropriate
26 programming of the Provisioning Server or by the MS vendor via appropriate
27 programming of the MS.
- 28 16) The IOTA Handset Configuration Management system SHALL be
29 implemented as a guaranteed and trusted delivery system. The MS SHALL
30 buffer all received data and respond to the Provisioning Server with a
31 “confirm” message to indicate that the MS has been successfully
32 programmed/updated. Failure of the Provisioning Server to receive the
33 “confirm” message SHALL be an indication that the operation failed and, at
34 the option of the service provider as specified in the programming of the
35 Provisioning Server, the operation SHALL be re-initiated at some point in
36 time in the future.

- 1 17) It is intended that handset and provisioning server implementations SHALL
2 be interoperable, as defined by later stages of the IOTA specifications.
- 3 18) If a service provider already has data transport services (i.e., C.S0017-0,
4 C.S0015-0, P.S0001-0, or Quick Net Connect), no changes will be necessary
5 to support IOTA Handset Configuration Management services. IOTA
6 SHALL only impact the MS and the Provisioning Server.
- 7 19) The HCM and MS SHALL support OTA provisioning of NAI Profile
- 8 20) IOTA SHALL support managing user specific IOTA objects in the R-UIM
9 when it is available.
- 10 21) The network operator or service provider SHALL validate the integrity of data
11 and applications provided to the mobile station via IOTA. The means or
12 procedures for validating the integrity of data or applications are beyond the
13 scope of the IOTA specifications.”

14 **6 Applicability to Telecommunications Services**

15 The IOTA Handset Configuration Management services are applicable to all
16 telecommunications services.

17 **6.1 Normal Procedures with Successful Outcome**

18 This section lists normal procedures to be followed which result in a successful outcome.

19 **6.2 Authorization**

20 IOTA Handset Configuration Management services are generally available to all current
21 subscribers of the service provider who have IOTA Handset Configuration Management
22 capable MS units.

23 **6.3 De-Authorization**

24 IOTA Handset Configuration Management services may be withdrawn by the service
25 provider.

26 **6.4 Registration**

27 IOTA Handset Configuration Management services have no registration.

28 **6.5 De-Registration**

29 IOTA Handset Configuration Management services have no de-registration.

30 **6.6 Activation**

31 IOTA Handset Configuration Management services have no activation.

32 **6.7 De-Activation**

33 IOTA Handset Configuration Management services have no de-activation.

34 **6.8 Invocation**

35 The MS user or the network may invoke IOTA Handset Configuration Management
36 services at any time. Mobile invocation may be restricted by appropriate programming of
37 the Provisioning Server. Network invocation may be restricted by appropriate

1 programming of the MS. The network should have a means of knowing if the MS is
2 IOTA-capable prior to invocation.

3 **6.9 Normal Operation with Successful Outcome**

4 This section describes a typical sequence of OTASP procedures for IOTA Handset
5 Configuration Management services. Similar sequences could be envisioned for
6 OTAPA, OTASD, and OTAMD. These procedures result in a successful outcome.

- 7 1. The network or the MS user invokes IOTA Handset Configuration Management
8 services with/using the target MS. No NAM selection is necessary (nor is it
9 possible) because, except in the case of an uninitialized MS invoking OTASP
10 operations, the MS has already identified which NAM is in use during
11 registration, and IOTA Handset Configuration Management services can be
12 performed only on the active NAM.
- 13 2. The network and the MS authorize one another using the SPASM. If this step
14 cannot be completed successfully, the MS shall immediately terminate the IOTA
15 Handset Configuration Management session.
- 16 3. The network transmits to the MS, or requests from the MS, the desired NAM,
17 data or other parameters over the air interface.
- 18 4. The MS commits the parameters received to permanent memory. The MS issues
19 the “commit” response to the Provisioning Server that indicates that the
20 programming operation has been successfully completed.
- 21 5. The MS resumes normal operation (with new parameters, if any) after the IOTA
22 Handset Configuration Management session is successfully completed.

23 **7 Exception Procedures or Unsuccessful Outcome**

24 This section lists some of the more probable abnormal situations not described in Normal
25 Procedures With Successful Outcome.

26 If the process of programming an MS terminates for any reason before the IOTA Handset
27 Configuration Management is successfully completed (i.e., MS commit response received
28 by the Provisioning Server), the MS shall return to the programmed information in effect
29 before the IOTA Handset Configuration Management procedure began.

30 **7.1 Registration**

31 None identified.

32 **7.2 De-Registration**

33 None identified.

34 **7.3 Activation**

35 None identified.

1 **7.4 De-Activation**

2 None identified.

3 **7.5 Invocation**

4 For network invoked operations, if the network is unable to successfully invoke IOTA
5 Handset Configuration Management services, there should be no indication to the user
6 nor should there be any effect on the user's ability to operate the MS.

7 **7.6 Exception While Roaming**

8 None identified.

9 **7.7 Exception During Intersystem Hand-off**

10 IOTA Handset Configuration Management procedures may be blocked during
11 intersystem handoff by the service provider, depending upon the specific implementation.

12 **8 Alternative Procedures**

13 None identified.

14 **9 Interaction With Other Services**

15 This section describes the interactions of the IOTA Handset Configuration Management
16 services with other standardized or proposed wireless telecommunication features.

17 **9.1 Standard Voice Services**

18 Simultaneous voice and data is strongly desired. This allows the customer care
19 representative to communicate with the user during IOTA operations.

20 **9.1.1 Call Delivery (CD)**

21 None identified.

22 **9.1.2 Call Forwarding-Busy (CFB)**

23 None identified.

24 **9.1.3 Call Forwarding-Default (CFD)**

25 None identified.

26 **9.1.4 Call Forwarding-No Answer (CFNA)**

27 None identified.

28 **9.1.5 Call Forwarding-Unconditional (CFU)**

29 None identified.

30 **9.1.6 Call Transfer (CT)**

31 None identified.

32 **9.1.7 Call Waiting (CW)**

33 None identified.

34 **9.1.8 Calling Number Identification Presentation (CNIP)**

35 None identified.

36 **9.1.9 Calling Number Identification Restriction (CNIR)**

37 None identified.

1 **9.1.10 Conference Calling (CC)**

2 None identified.

3 **9.1.11 Do Not Disturb (DND)**

4 None identified.

5 **9.1.12 Emergency Services**

6 For further study.

7 **9.1.13 Flexible Altering (FA)**

8 None identified.

9 **9.1.14 Message Waiting Notification (MWN)**

10 None identified.

11 **9.1.15 Mobile Access Hunting (MAH)**

12 None identified.

13 **9.1.16 Password Call Acceptance (PCA)**

14 None identified.

15 **9.1.17 Preferred Language (PL)**

16 The Provisioning Server may request the PL indicator setting from the MS and modify its
17 operations appropriately.

18 **9.1.18 Priority Access and Channel Assignment (PACA)**

19 For further study.

20 **9.1.19 Remote Feature Control (RFC)**

21 None identified.

22 **9.1.20 Selective Call Acceptance (SCA)**

23 None identified.

24 **9.1.21 Subscriber PIN Access (SPINA)**

25 None identified.

26 **9.1.22 Subscriber PIN Intercept (SPIN)**

27 None identified.

28 **9.1.23 Three-way Calling (3WC)**

29 None identified.

30 **9.1.24 Voice Message Retrieval (VMR)**

31 None identified.

32 **9.1.25 Voice Privacy (VP)**

33 None identified.

34 **9.1.26 Asynchronous Data Service (ADS)**

35 None identified.

36 **9.1.27 Calling Name Presentation (CNAP)**

37 None identified.

1 **9.1.28 Data Privacy (DP)**

2 None identified.

3 **9.1.29 Emergency Services Callback (E-9-1-1CB)**

4 None identified.

5 **9.1.30 Emergency Services Reconnect (E-9-1-1RC)**

6 None identified.

7 **9.1.31 Group 3 Facsimile Service (G3 FAX)**

8 None identified.

9 **9.1.32 Incoming Call Screening (ICS)**

10 None identified.

11 **9.1.33 Network Directed System Selection (NDSS)**

12 None identified.

13 **9.1.34 Non-Public Mode Service (NP)**

14 None identified.

15 **9.1.35 Over-the-Air Service Provisioning (OTASP)**

16 IOTA Handset Configuration Management services cannot be invoked while IS-683 type
17 OTA services are in progress.

18 **9.1.36 Speech Option Selection (SOS)**

19 None identified.

20 **9.1.37 User Group ID (UGID)**

21 None identified.

22 **9.1.38 Voice Controlled Services (VCS)**

23 None identified.

24 **9.1.39 IOTA Handset Configuration Management Services**

25 IOTA Handset Configuration Management services cannot be re-invoked while an IOTA
26 Handset Configuration Management operation is already in progress.

27 **9.1.40 ANSI-95 Service Programming Lock (SPL) or equivalent**

28 The SPL feature, when present and activated, prevents any modification of NAM
29 parameters without a valid Service Programming Code. The IOTA Handset
30 Configuration Management SPASM shall be independent of the SPL feature; that is,
31 deactivating SPL shall not affect the state of the SPASM, and vice versa.

32