

3GPP2 S.R0027

Version 1.0

Date: 8 December 2000



Personal Mobility

Stage 1 Requirements

COPYRIGHT

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.

Contents

Contents.....	2
1 Scope.....	4
2 References	4
2.1 Normative Reference.....	4
2.2 Informative References	4
3 Abbreviations.....	4
4 General.....	5
5 Personal Mobility Services	5
6 System Implications.....	5
6.1 Security.....	5
6.2 User Identity Information	7
7 Procedures for Personal Mobility Services.....	7
7.1 Normal Procedures With Successful Outcome.....	7
7.1.1 Authorization.....	7
7.1.2 De-Authorization.....	7
7.1.3 Registration.....	7
7.1.4 De-Registration.....	8
7.1.5 Activation.....	8
7.1.6 De-Activation.....	8
7.1.7 Invocation.....	8
7.1.8 Normal Operation with Successful Outcome.....	8
7.1.9 Call Detail Record.....	8
7.2 Exception Procedures or Unsuccessful Outcome.....	9
7.2.1 Registration.....	9
7.2.2 De-Registration.....	9
7.2.3 Activation.....	9
7.2.4 De-Activation.....	9
7.2.5 Invocation.....	9
7.2.6 Exceptions While Roaming.....	9
7.2.7 Exceptions During Intersystem Handoff.....	9
7.3 Alternate Procedures	10
7.3.1 Registration.....	10
7.4 Interactions With Other Cellular Services.....	10
7.4.1 Asynchronous Data Service (ADS).....	10
7.4.2 Call Delivery (CD).....	10
7.4.3 Call Forwarding—Busy (CFB).....	10

7.4.4	Call Forwarding—Default (CFD)	10
7.4.5	Call Forwarding—No Answer (CFNA)	10
7.4.6	Call Forwarding—Unconditional (CFU)	10
7.4.7	Call Transfer (CT)	10
7.4.8	Call Waiting (CW)	10
7.4.9	Calling Name Presentation (CNAP)	10
7.4.10	Calling Number Identification Presentation (CNIP)	10
7.4.11	Calling Number Identification Restriction (CNIR)	10
7.4.12	Conference Calling (CC)	11
7.4.13	Data Privacy (DP)	11
7.4.14	Do Not Disturb (DND)	11
7.4.15	Emergency Services Callback (9-1-1CB)	11
7.4.16	Emergency Services Reconnect (9-1-1RC)	11
7.4.17	Flexible Alerting (FA)	11
7.4.18	Global Emergency Call Origination (GECO)	11
7.4.19	Group 3 Facsimile (G3 FAX)	11
7.4.20	Incoming Call Screening	11
7.4.21	Message Waiting Notification (MWN)	11
7.4.22	Mobile Access Hunting (MAH)	11
7.4.23	Network Directed System Selection (NDSS)	11
7.4.24	Non-Public Mode Service (NP)	11
7.4.25	Over-the-Air Service Provisioning (OTASP)	11
7.4.26	Over-the-Air Parameter Administration (OTAPA)	11
7.4.27	Password Call Acceptance (PCA)	11
7.4.28	Preferred Language (PL)	12
7.4.29	Priority Access and Channel Assignment (PACA)	12
7.4.30	Remote Feature Control (RFC)	12
7.4.31	Selective Call Acceptance (SCA)	12
7.4.32	Service Programming Lock (SPL)	12
7.4.33	Speech Option Selection (SOS)	12
7.4.34	Subscriber PIN Access (SPINA)	12
7.4.35	Subscriber PIN Intercept (SPINI)	12
7.4.36	Three-Way Calling (3WC)	12
7.4.37	Tiered Services (TS)	12
7.4.38	User Group ID (UGID)	12
7.4.39	Voice Controlled Services (VCS)	12
7.4.40	Voice Message Retrieval (VMR)	12
7.4.41	Voice Privacy (VP)	12

1 Scope

The objective is to define and standardize the functionality of personal mobility that can be incorporated into the operations of both 2G/3G TIA/EIA-41 and 2G/3G GSM-derived wireless telecommunications networks. This document defines the requirements of personal mobility features and services.

2 References

2.1 Normative Reference

- S.R0001 – 3GPP2 Specifications List
- S.R0002 – 3G Capability Descriptions

2.2 Informative References

-

3 Abbreviations

For the purpose of this document, the following abbreviations apply:

3G	Third Generation system
3GPP2	Third Generation Partnership Project 2
FER	Frame Error Rate
ISO	International Standards Organization
ITU-T	International Telecommunication Union - Telecommunication Sector
ME	Mobile Equipment
MS	Mobile Station, a ME with a UIM
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request for Comments
RLP	Radio Link Protocol
SIP	Session Initiated Protocol
TIA	Telecommunications Industry Association
UIM	User Identity Module
R-UIM	Removable User Identity Module
U-UIM	Universal UIM

4 General

Wireless personal mobility allows a user to access telecommunication services at any wireless terminal¹ based on unique user identity and security information. A single international mobile subscriber identity provides the uniqueness for each set of user identity and security information.

Wireless personal mobility encompasses two aspects:

- (1) the transfer of unique user identity and security information to a designated mobile station in a home or other family system type.
- (2) the authentication and location registration of a mobile station in an other family system type. The mobile station will already be in possession of a unique set of user identity and security information.

The user is provided those services delineated in their service profile within the limits of the wireless terminal and serving system. The user is not required to know which family system types of wireless networks are serving the user's location.

A terminal will not be available for wireless personal mobility service unless authorized by the terminal owner.

5 Personal Mobility Services

Wireless personal mobility is applicable to voice and data telecommunications services. The full range of bearer services available at a given location will be available to the wireless personal mobility user (subject to the network and terminal limitations)

6 System Implications

6.1 Security

The Universal UIM (U-UIM) supports a variety of methods for the performance of user authentication and key agreement. These methods are specified for each air interface access technology. In particular, the U-UIM supports the 3GPP Authentication and Key Agreement (AKA) method as specified in draft 3G TS 33.102. It is anticipated that this method will become the preferred AKA technique for all wireless technologies as systems evolve towards 3G operation.

¹ The wireless terminal must have personal mobility capability.

It may also be necessary for the U-UIM to also support 2G technologies, such as those developed by the TIA in North America for ANSI-136 (tdma access) and ANSI-95 (cdma access). Additionally, some 3G technologies may include embellishments on the basic AKA scheme.

To ensure that the U-UIM support multiple, distinct, access technologies, it will be necessary that its security architecture be carefully specified. On one extreme, the U-UIM might contain a distinct set of all functions and parameters for each technology. On the other extreme, it might contain a minimal set of functions and parameters as required for a small set of similar technologies, coupled with some means to translate access messages and parameters to satisfy the requirements of other access technologies.

In another solution, the U-UIM might contain two disjoint sections, one that performs the GSM/UMTS functions, and one that performs the ANSI-136/ANSI-95 set of functions. In the GSM/UMTS section, the U-UIM stores a key denoted "K" and a set of authentication-related algorithms such as "A3/A8" and "f0 through F5." In the ANSI-standard section, the U-UIM stores an "A-key", "SSD" and the authentication and key calculation methods as specified in ANSI 2G standards.

The extent to which translations are used to minimize U-UIM access network computational loading and parameter storage need to be determined. In the example cited above, it seems reasonable that the GSM/UMTS section could easily translate security parameters such as Ck and Ik into Kc. Formal specification of these translations is underway in 3GPP TSG-A WP3. Similarly, it seems reasonable that functions and parameters (such as an A-key) might be re-used across ANSI-specified access technologies.

The issue to be resolved, therefore, is whether the network will be configured to provision U-UIMs with both sets of parameters, i.e., "A-key" and ANSI-related security functions, along with "K" and GSM/UMTS security functions or whether a network be configured to provision their U-UIMs with one set of parameters along with one or more translation functions that would provide access to the air interface access technologies.

In both cases the network infrastructure elements would need to support all modes of signaling so that procedures such as location updates and call processing might be accommodated across multiple air interface access technologies. The ability to support universal roaming already requires cross-technology message and parameter translation, it seems reasonable that the translation of security-related messages and parameters would also be desired.

It is therefore required that both the U-UIM and compatible networks should support the translation of security-related functions and parameters so that one preferred set of security data may be provisioned in the network.

6.2 User Identity Information

The user may store their set(s) of user identity and security information:

- on an integrated circuit or integrated circuit card that is not removable from a mobile terminal
- on an integrated circuit card that is removable from a mobile terminal
- in the network with the service provider
- or any combination of the above.

Each unique set of user identity and security information may be active at only one terminal simultaneously (uniqueness provided by the user's international mobile subscriber identity). The user may designate a terminal to which their set(s) of user identity and security information may be transferred from the network over the air. The user may transfer their set(s) of user identity information to a designated terminal by transferring a removable integrated circuit card from one terminal to another.

Multiple sets of user identity information may be stored on removable or non-removable integrated circuit cards or within the network. Multiple removable integrated circuit cards may be input into a single terminal.

7 Procedures for Personal Mobility Services

7.1 Normal Procedures With Successful Outcome

This section describes the normal procedures that result in a successful outcome.

7.1.1 Authorization

Wireless personal mobility may be generally available or may be provided after pre arrangement with the service provider.

7.1.2 De-Authorization

Wireless personal mobility may be withdrawn at the subscriber's request or the service provider's request

7.1.3 Registration

Wireless personal mobility shall be registered when a set of user identity and security information is transferred to a designated MS. The set of user identity and security information is transferred over the air. User actions to accomplish over the air transfer are Non identified. See Alternate Procedures for other registration methods

7.1.4 De-Registration

Wireless personal mobility shall be de-registered when a set of user identity and security information is removed from a designated MS.

7.1.5 Activation

Wireless personal mobility shall be activated when a wireless location registration with a user's unique set of user identity and security information is performed.

7.1.6 De-Activation

Wireless personal mobility shall be de-activated upon de-authorization. Wireless personal mobility may be automatically de-activated when inactivity reporting is performed for an authorized subscriber.

7.1.7 Invocation

Wireless personal mobility is invoked when there is an incoming call or call origination or other service profile feature invocation, wireless personal mobility is registered, and wireless personal mobility is active.

7.1.8 Normal Operation with Successful Outcome

When wireless personal mobility is invoked:

1. incoming calls shall be directed to the system serving the subscriber. Call delivery treatment will be influenced by the subscriber's profile. For example, additional calls would not be delivered to a user engaged in a call unless they are subscribed to Call Waiting.
2. originated calls will be influenced by the subscriber's profile
3. services normally available to the subscriber in their home system will be made available to the subscriber in a visited serving system subject to the network and terminal restrictions

7.1.9 Call Detail Record

The system should record call detail information for the following against the subscriber's international mobile subscriber identity.

- a. Visited system registration activities and events.
- b. Home system registration activities and events.
- c. Power-down de-registration activities and events.
- d. Visiting system inactivity reporting activities and events.
- e. Wireless personal mobility activation activities and events.
- f. Wireless personal mobility de-activation activities and events.

- g. Wireless personal mobility invocation events.
- h. Call delivery leg usage.
- i. Call origination usage.
- j. No MS response to a page request.
- k. No MS or subscriber response to alerting.
- l. No subscriber response to Call Waiting notification.
- m. Feature usage duration.

7.2 Exception Procedures or Unsuccessful Outcome

This section describes abnormal situations not described in "Normal Operation with Successful Outcome."

7.2.1 Registration

None identified.

7.2.2 De-Registration

None identified.

7.2.3 Activation

If the subscriber is not authorized for the request, the system shall apply denial call treatment when activation is attempted.

7.2.4 De-Activation

None identified.

7.2.5 Invocation

None identified.

7.2.6 Exceptions While Roaming

None identified.

7.2.7 Exceptions During Intersystem Handoff

None identified.

7.3 Alternate Procedures

7.3.1 Registration

Wireless personal mobility shall be registered when a set of user identity and security information is transferred to a designated mobile terminal. Inserting an integrated circuit card containing a unique set of user identity and security information transfers the information. See Normal Procedures for another registration method.

7.4 Interactions With Other Cellular Services

This section describes the interaction of Personal Mobility with other cellular services when more than one cellular feature is active.

7.4.1 Asynchronous Data Service (ADS)

Non identifiedNon identified.

7.4.2 Call Delivery (CD)

Non identifiedNon identified.

7.4.3 Call Forwarding—Busy (CFB)

Non identifiedNon identified.

7.4.4 Call Forwarding—Default (CFD)

Non identifiedNon identified.

7.4.5 Call Forwarding—No Answer (CFNA)

Non identified.

7.4.6 Call Forwarding—Unconditional (CFU)

Non identified.

7.4.7 Call Transfer (CT)

Non identified.

7.4.8 Call Waiting (CW)

Non identified.

7.4.9 Calling Name Presentation (CNAP)

Non identified.

7.4.10 Calling Number Identification Presentation (CNIP)

Non identified.

7.4.11 Calling Number Identification Restriction (CNIR)

Non identified.

7.4.12 Conference Calling (CC)

Non identified.

7.4.13 Data Privacy (DP)

Non identified.

7.4.14 Do Not Disturb (DND)

Non identified.

7.4.15 Emergency Services Callback (9-1-1CB)

Non identified.

7.4.16 Emergency Services Reconnect (9-1-1RC)

Non identified.

7.4.17 Flexible Alerting (FA)

Non identified.

7.4.18 Global Emergency Call Origination (GECO)

Non identified.

7.4.19 Group 3 Facsimile (G3 FAX)

Non identified.

7.4.20 Incoming Call Screening

Non identified.

7.4.21 Message Waiting Notification (MWN)

Non identified.

7.4.22 Mobile Access Hunting (MAH)

Non identified.

7.4.23 Network Directed System Selection (NDSS)

Non identified.

7.4.24 Non-Public Mode Service (NP)

Non identified.

7.4.25 Over-the-Air Service Provisioning (OTASP)

Non identified.

7.4.26 Over-the-Air Parameter Administration (OTAPA)

Non identified.

7.4.27 Password Call Acceptance (PCA)

Non identified.

7.4.28 Preferred Language (PL)

Non identified.

7.4.29 Priority Access and Channel Assignment (PACA)

Non identified.

7.4.30 Remote Feature Control (RFC)

Non identified.

7.4.31 Selective Call Acceptance (SCA)

Non identified.

7.4.32 Service Programming Lock (SPL)

Non identified.

7.4.33 Speech Option Selection (SOS)

Non identified.

7.4.34 Subscriber PIN Access (SPINA)

Non identified.

7.4.35 Subscriber PIN Intercept (SPINI)

Non identified.

7.4.36 Three-Way Calling (3WC)

Non identified.

7.4.37 Tiered Services (TS)

Non identified.

7.4.38 User Group ID (UGID)

Non identified.

7.4.39 Voice Controlled Services (VCS)

Non identified.

7.4.40 Voice Message Retrieval (VMR)

Non identified.

7.4.41 Voice Privacy (VP)

Non identified.