Network Working Group
Request for Comments: 2636
Obsoletes: 2604
Category: Informational

R. Gellens
Qualcomm
July 1999

Wireless Device Configuration (OTASP/OTAPA) via ACAP

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Abstract

Wireless carriers today are faced with creating more efficient distribution channels, increasing customer satisfaction, while also improving margin and profitability. Industry trends are pushing the sale of handsets further into the retail channel. The cost and effort of provisioning handsets, activating users, and updating handset parameters can be greatly reduced by using over-the-air activation mechanisms. A comprehensive and extensible means for over-the-air provisioning and handset parameter updating is required.

One approach is to purchase EIA/TIA/IS-683A (Over-the-air Service Provisioning of Mobile Stations in Spread Spectrum Systems) equipment. The cost of this has led carriers to seek alternative solutions. A very viable means for providing over-the-air (OTA) provisioning is to leverage the rollout of IS-707 data services equipment, which most carriers are in the process of deploying. This paper presents an approach to OTA provisioning that utilizes the deployment of IS-707 to deliver OTA provisioning and parameter upgrading.

IS-707 data services makes available several methods of providing over-the-air provisioning and parameter updating. A well thought-out approach utilizing Internet-based open standard mechanisms can provide an extensible platform for further carrier service offerings, enhanced interoperability among back-end services, and vendor independence.

This paper describes a viable and attractive means to provide OTASP/OTAPA via IS-707, using the ACAP[ACAP] protocol.

Table of Contents

1. Terms

Application Configuration Access Protocol (ACAP) – An Internet protocol (RFC-2244) that provides remote storage and access of configuration and preference information.

Activation – A process in which a mobile station and network become programmed so that a mobile station becomes operable and can be used for cellular service once authorized by the service provider.

Authentication – A procedure used to validate a mobile station's identity.

Authentication Center – An entity that manages the authentication information related to the mobile station.

Authentication Key (A-key) – A secret 64-bit pattern stored in the mobile station. It is used to generate and update the mobile station's shared secret data. The A-key is used in the authentication process.

Authorization – An action by a service provider to make cellular service available to a subscriber.

Call – A temporary communication between telecommunications users for the purpose of exchanging information. A call includes the sequence of events that allocates and assigns resources and signaling channels required to establish a communications connection.

Cellular Service Provider – A licensee of the responsible government agency (in the U.S. a licensee of the Federal Communications Commission) authorized to provide Cellular Radiotelephone Service.

Challenge/Response Authentication Mechanism using Message Digest 5 (CRAM-MD5) – An authentication mechanism which is easy to implement, and provides reasonable security against various attacks, including replay. Supported in a variety of Internet protocols. Specified as baseline mechanism in ACAP. CRAM-MD5 is published as RFC 2195.

Code Division Multiple Access – A technique for spread-spectrum multiple-access digital communications that creates channels through the use of unique code sequences.

Customer Service Center – An entity of a service provider that provides user support and assistance to subscribers.

Customer Service Representative – A person that operates from a customer service center and provides user support and assistance to subscribers.

Diffie-Hellman Algorithm – A public-key cryptography algorithm for exchanging secret keys. Uses the equation $k = g^{xy} \bmod p$, where k is the secret key. The equation is executed by each party of the session based on the exchange of independently generated public values.

Digits – Digits consist of the decimal integers 0,1,2,3,4,5,6,7,8, and 9.

Dual-mode Mobile Station – A mobile station capable of both analog and digital operation.

Electronic Serial Number (ESN) – A 32-bit number assigned by the mobile station manufacturer used to identify a mobile station. The ESN is unique for each legitimate mobile station.

Home Location Registry (HLR) – The location register or database to which a MIN is assigned for record purposes such as subscriber information.

Message Digest 5 (MD5) – A one-way cryptographic hash function. Widely deployed in Internet protocols. Published as RFC 1321.

Mobile Identification Number (MIN) – The 10-digit number that represents a mobile station's directory number.

Mobile Station (MS) – A station, fixed or mobile, which serves as the end user's wireless communications link with the base station. Mobile stations include portable units (e.g., hand-held personal units) and units installed in vehicles.

Mobile Switching Center (MSC) – A configuration of equipment that provides cellular radiotelephone service.

Mobile Terminal Authorizing System (MTAS) – A control system that provides the capability to load the CDMA network HLR with mobile station profile information.

Number Assignment Module (NAM) – The mobile station's electronic memory module where the MIN and other subscriber-specific parameters are stored. Mobile stations that have multi-NAM features offer users the option of using their units in several different markets by registering with a local number in each location.

Over-the-air Service Provisioning Function (OTAF) – A configuration of network equipment that controls OTASP functionality and messaging protocol.

Over-the-air Parameter Administration (OTAPA) – Network initiated OTASP process of provisioning mobile station operational parameters over the air interface.

Over-the-air Service Provisioning (OTASP) – A process of provisioning mobile station operational parameters over the air interface.

Quick-Net-Connect (QNC) – An IS-707 data service capability that utilizes the Async Data Service Option number but bypasses the modem connection for a direct connection to an IP-based internet.

Roamer – A mobile station operating in a cellular system or network other than the one from which service was subscribed.

Simple Authentication and Security Layer (SASL) – An Internet protocol (RFC-2222) that provides a framework for negotiating authentication and encryption mechanisms.

Service Provider – A company, organization, business, etc. which sells, administers, maintains, and charges for the service. The service provider may or may not be the provider of the network.

Shared Secret Data (SSD) – A 128-bit pattern stored in the mobile station (in semi-permanent memory) and known by the network. The A-key is used to generate the SSD at the network and in the mobile station for comparison.

Wireless Application Protocol (WAP) – A set of network and application protocols including a datagram protocol (WDP), Transport Layer Security (WTLS), Transaction Protocol (WTP), Session Protocol (WSP), and Application Environment (WAE), which use carrier-based gateways to enable wireless devices to access Web resources. See <http://www.wapforum.org> for specifications and details.

2. Feature Descriptions

2.1 OTASP Feature Description

The Over the Air Service Provisioning (OTASP) feature allows a potential wireless service subscriber to activate new wireless services, and allows an existing wireless subscriber to make services changes without the intervention of a third party. OTASP includes the following:

- A way to establish a user profile.
- "Over-The-Air" programming of a Number Assignment Module (NAM), IMSI and Roaming Lists, including Data option parameters, and optionally, service provider or manufacturer specific parameters (e.g., lock code, call timer).
- An Authentication Key (A-key) Generation procedure.
- A-key storage

2.2 OTAPA Feature Description

The Over-the-Air Parameter Administration (OTAPA) feature allows wireless service providers to update a NAM, IMSI, and Roaming List information in the mobile station remotely without the intervention of a third party. This capability increases flexibility and reduces costs for carriers involved with mass changes that affect every handset, such as area-code splits.

OTAPA includes the following:

- Update a user's Number Assignment Module (NAM)
- Update Data option parameters
- Update service provider or manufacturer specific parameters (e.g., Server address(es), lock code, call timer).
- Update roaming lists

3. Operation

3.1 Initial Provisioning Activity

A new subscriber needs to give the intended service provider sufficient information (e.g., name, address, etc.) to prove credit-worthiness and establish a record within the service provider's billing system. In addition, the ESN of the mobile station needs to be given to the provider. This may occur in three ways:

Voice scenario — A customer care representative collects credit information during a voice conversation. This call is made from a different phone (e.g., wired service) or is initiated using the IS-683A OTASP dialing scheme (i.e., *228*xx*).

Once the user has been authorized, the customer care representative creates a record in the CDMA network HLR, thus allowing use of the CDMA network. In addition, a limited-time N-digit password is created which is tied to the ESN. The choice of N (how many digits) is up to the carrier (as a trade-off between security and user inconvenience). All required provisioning information (including the limited-time password) is loaded into the provisioning server.

The user is then told to hang up and call a special number, of the form *228 XX <*N-digit password*> SEND (the XX code is the same as used in the initial voice call). This causes the mobile station to initiate a provisioning session.

The mobile station and the provisioning server authenticate, and all required provisioning information is downloaded into the mobile station. The user receives some form of notification once the activity is complete. This notification can be an audible tone or a text message on the mobile station display. (The form and content of this notification can be part of the provisioning data downloaded by the mobile station.) Once this initial provisioning activity is complete the user has a fully authorized mobile station ready for use.

Forms scenario — An interactive user interface is presented via a browser on the mobile station. The subscriber fills in the requested information. (Note that entering non-numeric data presents some user interface challenges on many mobile devices.)

A back-end server validates the information, and if possible, the customer is authorized, a limited-time password is generated, HLR and provisioning server records are created and the actual OTASP operation begins. Otherwise, a voice call is made to a customer care representative.

Desktop scenario — The subscriber uses a desktop (or in-store kiosk) web browser to contact the carrier, and enters the usual personal information.

The carrier's server validates the information, and if possible, the customer is authorized, a limited-time password is generated, HLR and provisioning server records are created, and the subscriber is told to dial a special number on the handset. Once this code is entered, the actual OTASP operation begins. Otherwise, the user is asked to make a voice call to a customer care representative.

3.2 OTASP for Authorized Users

Users already authorized for use of the CDMA network can also initiate provisioning activity. This could happen after being directed to do so by a Customer Care representative, either from a phone conversation or via mail notification. This type of OTASP activity is needed in cases where the carrier desires to upgrade CDMA parameters in the mobile stations or in cases where mobile station troubleshooting is needed.

This type of OTASP occurs in similar fashion to the initial OTASP activity. The mobile station downloads the new provisioning information in the same way.

3.3 OTAPA Activity

Typical OTAPA capability involves upgrading a large number of mobile stations. OTAPA activity needs to be performed in a manner that does not impose on revenue bearing CDMA network activity. OTAPA operations are initiated at the customer care center. This can be accomplished by queuing a notification to the mobile station (via 1-way SMS or special caller-ID) after the provisioning server has the updated configuration data. OTAPA activity will not occur until the mobile station has acquired CDMA service on the carrier's network and the notification has reached the mobile station.

Alternatively, OTAPA can be handled by including a recheck interval in the set of data used to provision the mobile station. When using a low-overhead protocol, such as ACAP [ACAP], it is reasonable to have a mobile station check in periodically to see if anything has changed. The time of day and/or day of week that such rechecks should occur could be included in the provisioning data.

OTAPA activity can be terminated at any time due to user call activity.

4. Requirements

4.1 General Requirements

IS-683A OTASP operations occur between a mobile station and an over-the-air service provisioning function (OTAF) using IS-95A traffic channel data burst messages. OTASP/OTAPA via data services require that the CDMA carrier have an IS-707 data services capable network. The IS-707 service must be either Packet Data Service (IS-707.5) or Quick-Net-Connect (QNC).

The mobile station must support:

- IS-707 Data Service capability
- Packet/QNC RLP protocol
- PPP protocol to peer to the IS-707 IWF
- IP protocol to provide the network layer for routing to the provisioning server
- A transport layer for end-to-end communication (such as TCP)
- Authentication and optionally encryption
- Application software to handle the provisioning protocol and memory access.
- Domain Name System (DNS) query capabilities sufficient to obtain the (IP) address of the provisioning server (or the provisioning server’s address could be provided during PPP negotiation).

Lastly, the ability must exist for the mobile to make a data call and (optionally) a voice call without a MIN.

4.2 OTASP Requirements

The OTASP function requires the mobile station to originate an IS-707 data call and (optionally) a voice call using a completely unprovisioned mobile station. The CDMA network must support this capability.

OTASP via data services uses a provisioning server that contains the parameter information for mobile stations. The authorizing agent (or software) at the customer care center must be able to add user and mobile station information into both the CDMA network HLR and the provisioning server during the initial authorizing process. The provisioning server must be capable of servicing a mobile as soon as its record is created.

4.3 OTAPA Requirements

IS-683A OTAPA is performed by a mobile-terminated call that downloads parameters to the mobile station. OTAPA calls occur without user interaction.

In order to perform OTAPA via data services the network needs to direct the mobile station to initiate a special-purpose data call. Several existing methods can be used to implement this capability, for example, a mobile-terminated one-way SMS message. The SMS message content can contain any information required by the mobile station. The mobile station would need a simple parser of SMS messages in order to know when to originate an OTAPA call, as opposed to normal SMS message processing. The OTAPA call would be performed in similar fashion to a registration call. More specifically, the user would not be informed of the call activity.

There are alternative means that can be employed to initiate OTAPA activity; for example, a mobile-terminated voice call with caller-ID using a specialized telephone number. Another alternative is for mobile stations to periodically check in with the provisioning server to check for updated information. ACAP, for example, is designed for such a model. The recheck interval, as well as the time of day and/or day of week that such checks should be used, can be part of the provisioning data sent to the mobile stations.

4.4 Provisioning Server Requirements

IS-683A utilizes an over-the-air service provisioning function (OTAF) to perform the network-side provisioning activity. OTASP/OTAPA via data services replaces the OTAF with a provisioning server. The provisioning server resides on an IP network within the controlled confines of the carrier. The provisioning server must perform all the service provisioning and parameter administration functions that the OTAF provides. The provisioning server must also have an interface to the carrier’s Mobile Terminal Authorizing System (MTAS). This interface serves to synchronize the provisioning server with the information in the MTAS. The specific requirements of this interface depend on the capabilities and interfaces of the carrier’s customer care center system(s). The provisioning server must be capable of receiving dynamic updates from the MTAS and have the provisioning information immediately available for downloading into the chosen mobile station. A standard ACAP server provides an excellent means to meet these requirements.

The provisioning server must be capable of performing an authentication procedure with the mobile station. This authentication mechanism must be capable of authenticating both the mobile station and the provisioning server.

4.5 Security Requirements

OTASP requires that an authentication procedure be performed to validate the mobile station to the provisioning server, while OTAPA requires a mechanism where the mobile validates the server.

The provisioning server must be capable of either:

- OTAF A-key generation using a Diffie-Hellman mechanism

Or:

- Receiving A-keys from the carrier network.

Since data OTASP/OTAPA operates over IP within the carrier's network, end-to-end encryption between the mobile station and the provisioning server should be considered as a future enhancement. End-to-end encryption protects against attacks from within a carrier's network, and safeguards the provisioning data (for example, roaming lists).

5. Architecture

5.1 ACAP over TCP/IP

Figure 1 shows a provisioning server in the carrier's intranet which supports the Application Configuration Access Protocol (ACAP, RFC 2244). An administrative client in the customer care domain updates this server using ACAP. Handsets are provisioned and configured using a small ACAP client.

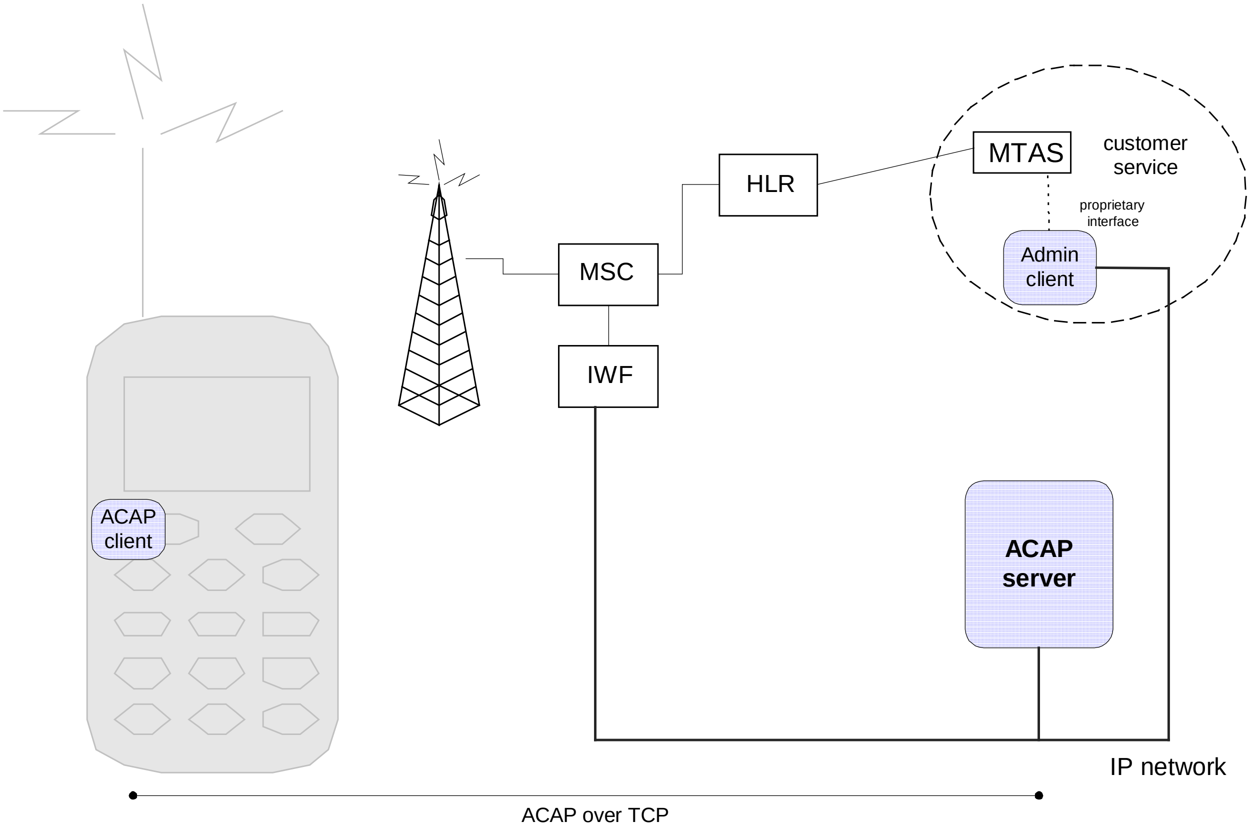

Figure 1

ACAP is an open Internet protocol designed to solve the problem of client access to configuration and related data. Among its primary goals are protocol simplicity, support for thin clients, and ease of operation over limited bandwidth. ACAP provides a high degree of extensibility, especially in authentication mechanisms, specialized attribute handling, and data management.

5.1.1 Mobile Authentication and A-Key Generation

The mobile client authenticates with the ACAP server prior to performing any activities. Authentication uses the mobile’s ESN and a shared secret. Provisioned mobiles derive the shared secret from the A-Key; unprovisioned mobiles use a limited-time password