*A well designed P&A technique is necessary to protect assets*

# Techniques for Privacy and Authentication in Personal Communication Systems

**DAN BROWN**

Personal Communication Systems (PCS) are anticipated to bring ubiquitous wireless telephony into widespread public use. To help further this goal, system designers are pursuing solutions to a number of challenges. These include accommodations for terminal (handset) mobility, personal mobility, universal roaming, access control, and the protection of user information sent via the airwaves. Of these, the latter two are often considered as a single subsystem called "Privacy and Authentication" (P&A). A well-designed P&A technique is necessary to protect assets. Network assets are protected by the access control (authentication) portion which enables legitimate users to utilize network services for which they have subscribed, while denying service to "hackers" who would steal services and monopolize resources. Subscriber assets (e.g., confidential information) are protected by encryption of traffic (privacy) on the radio link.

Authentication and privacy are generally linked together because the derivation of a "session key" for an encryption algorithm is often an integral part of the authentication process. From a designer's perspective, the access control and derivation of a session key form a single activity called Authentication and Key Agreement (AKA). The subsequent use of this session key to achieve encryption of user traffic can then be treated as a separate topic. This includes the selection of a cryptographic algorithm having properties that are compatible with the air interface to be protected.

This work describes progress to date in the development of AKA processes for PCS. A conceptual framework is first established; this is a three-part general model that characterizes all AKA techniques. Then three proposed AKA methods are compared using this model. These methods are the so-called secret key method of GSM, the secret key method of United States Digital Cellular (IS-54, IS-95), and a public key/secret key method that has been recently described in technical literature. Finally, a summary is presented that indicates the AKA method of preference for some proposed PCS air interfaces that are currently under development by standards bodies.

## A General Model for Access Control (Authentication and Key Agreement)

Figure 1 depicts the general AKA process. The user's handset is shown on the upper-left side as a "flip-phone," and the service provider's network is shown as a cloud-like shape in the upper-right corner. Most security methods are initiated when the user purchases a phone, and continue toward the goal of protecting the user's traffic through encipherment over the wireless media. These endpoints are depicted at the top and bottom, respectively, in Fig. 1. The three-part security model that connects these endpoints provides the logical steps necessary to accomplish this process. These parts are described below. Three composite P&A methods are later compared through the use of this model.

The first part of the general security model is Provisioning. This is the means by which a handset or user acquires the bona fides that will enable the network to subsequently recognize him as a legitimate user. It is essential that these bona fides permit the user access to the network while frustrating any "hacker" who attempts access "replays" or false interrogation of the handset.

Part two of the model is the means by which a handset establishes credibility when the user registers with a local service provider who is generally not the "home" network. In such cases, a local service provider should only acquire a byproduct or subset of handset credentials. This is necessary in a well-planned P&A method because any promulgation of handset secrets will eventually result in their compromise. However, it is still necessary that the local network be capable of distinguishing a legitimate user, based on partial security information.

The third part of the model is the protocol that is executed to permit network access and establish a key for protection of channel traffic. In secret key systems, this is generally a simple challenge/response mechanism. Public-key systems typically use the exchange of "certificates" and modulo-exponentiation to complete the AKA transaction.

## Comparison Process

These three processes will each be examined for PCS P&A proposals that are based upon GSM, IS-41, and a Public Key method. The purpose of this comparison is to highlight some differences of the three methods without attempting to assign quantitative values. The reader is encouraged to consult the references for more detailed information.

Because the GSM and IS-41 proposals are quite similar, the comparison process will be completed for these methods on a side-by-side basis. This is illustrated in Figs. 2, 3, and 4. Then the Public Key method will be described in order to contrast it to both secret key methods. The public-key method is shown in condensed form as Fig. 5.


1070-9916/95/$04.00 © 1995 IEEE

## Provisioning in Secret Key Systems

Refer to Fig. 2. The upper portion shows that in GSM-style systems, the service provider controls the security process by issuing a "Subscriber Identity Module" (SIM) to the user. A SIM often takes the form of a credit card-like device intended for insertion in the handset. The SIM contains information about the services that have been purchased, and it also contains a 128-bit number called "Ki" that is unique for each SIM. Ki enables the SIM to authenticate itself to the network. When the service provider issues the SIM to the user, he also must store Ki in a secure manner at the network. A loss of Ki's at the network could result in widespread fraudulent access due to user impersonations. In GSM-style systems, Ki's never leave the network of the "home" service provider.

In the United States, IS-41-based digital wireless telephony evolved from the AMPS analog cellular system. IS-41 refers to the network signaling protocol; its companion digital air interface standards in the cellular spectrum are IS-54 (TDMA) and IS-95 (CDMA). In all current IS-41-based systems, subscriber-specific information is downloaded into a user's handset by electronic means, generally by a service shop that is authorized to perform this function by the service provider.

The practice of using a removable SIM has not been a component of the analog-to-digital evolution in the United States The introduction of security features into IS-54, IS-95, and later into AMPS and NAMPS has instead relied upon a method by which the user enters a security parameter called the "A-Key" into his handset via the keypad. This technique begins when the service provider sends the 64-bit A-Key to the user in a confidential manner, such as through the U.S. mail. This direct link between the user and the service provider is intended to bypass the service shop, which can be a source of fraud through either intentional or careless mishandling of security information. The user's correct entry of the A-Key is verified by security software within the handset. It is also necessary that the service provider store the user's A-Key at the "home" network. Provisioning of the A-Key is shown in the lower section of Fig. 2. The A-Key never leaves the "home" network, just as Ki never leaves its GSM "home" network.

Establishment of an A-Key is the first of two components of IS-41 security provisioning. A second security variable called the "Shared Secret Data" is derived from the A-Key by means of an over-the-air protocol that can be initiated by only the home service provider. SSD is intended to be shared between a home network and a visited network in order that the handset can be autonomously authenticated by the visited network. This feature is further discussed in the next section.

## Access Control

The previous section describes how the "home" service providers in both GSM and IS-41 systems establish unique secrets with each subscriber. Mutual knowledge of these secrets enables the respective network to authenticate its

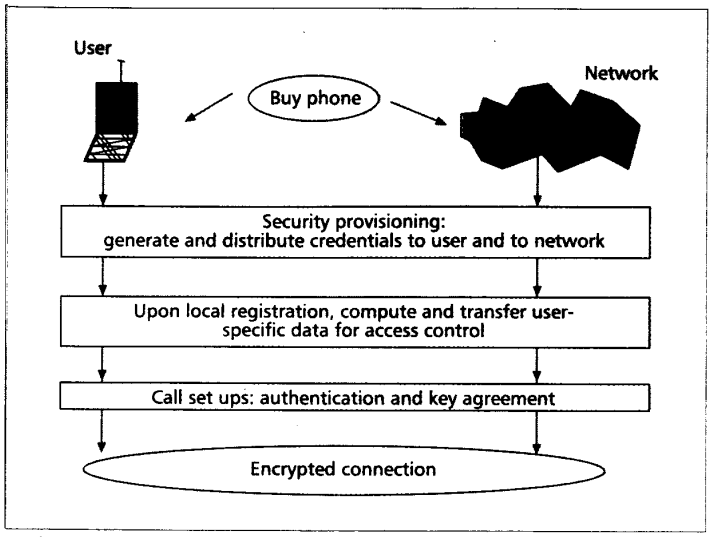


**Figure 1.** *AKA process: a general model.*

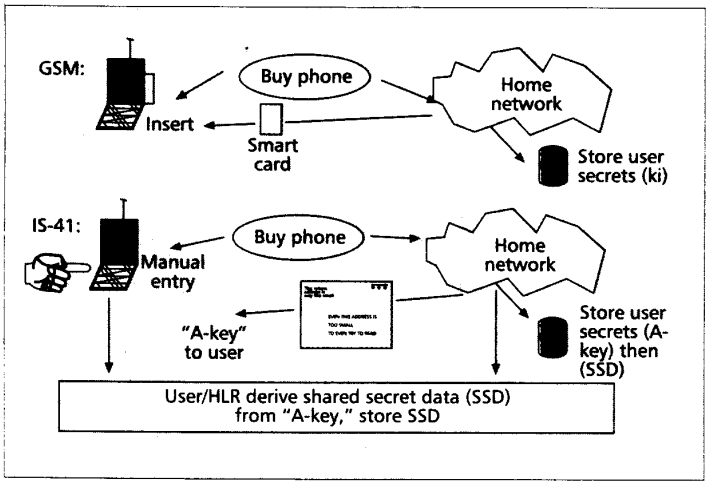


**Figure 2.** *P&A provisioning of secret key systems.*

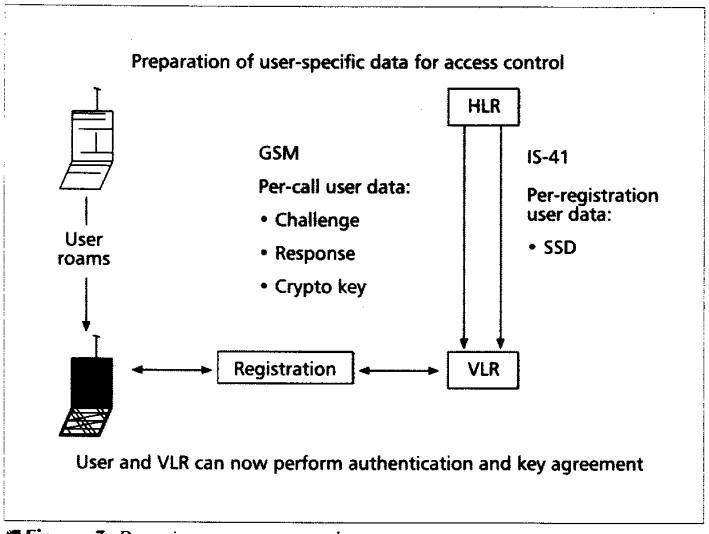


**Figure 3.** *Roaming support: secret key systems.*

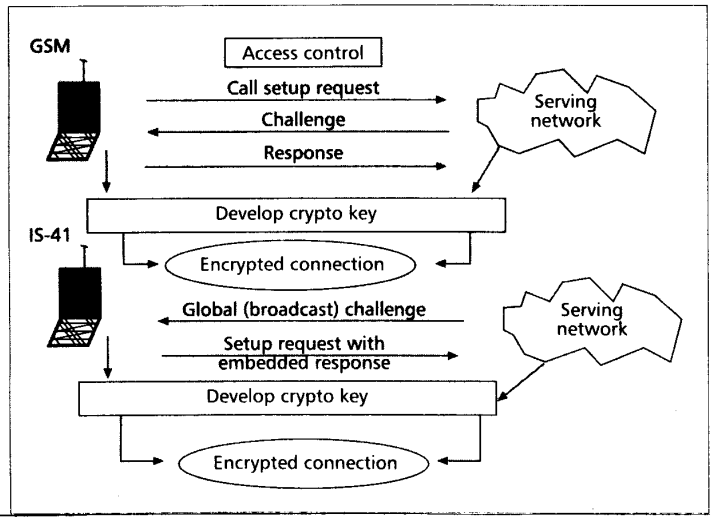


**Figure 4.** *AKA protocols: secret key systems.*

users when service is requested. However, terminal mobility permits the handset to be carried into the service areas of other, "visited" networks. This is also called "roaming," and business agreements are generally negotiated between service providers to support each other's roaming users. This results in a dilemma for the authentication process. A sufficient amount of information must be supplied to the visited network to authenticate a roamer, but this information must not be adequate to enable someone at the visited site to permanently impersonate a legitimate subscriber. The local network must be capable of performing authentication, but the process must be controlled by the home network.

The process of access control in a roaming situation is depicted in Fig. 3. A handset shown on the left side of the figure has roamed from its home network, served by its Home Location Register (HLR), to another network, where it will be served by the (other network's) Visited Location Register (VLR). An authentication will be performed upon handset registration with the VLR. Two flows of information are shown from the HLR to the VLR in order to support the authentication. The left-hand side depicts the information content that is supplied in GSM-style systems, while the right-hand side shows the information that is provided in IS-41-style systems.

In GSM-style systems, roaming subscribers are supported by their HLR in the form of "triplets" that provide security information to the VLR without revealing the secret Ki. Each set of triplets consists of a subscriber-unique random challenge RAND, an expected response SRES, and a resulting cipher key Kc. The number of triplets sent in a package may vary, but sets of five are common. Triplets are sent upon registration and thereafter as needed for the duration of the user's visit to the VLR's service area. The use of triplets permits the VLR to authenticate the roamer and establish a cipher key, but unauthorized interception of triplets does not enable permanent impersonation of a legitimate subscriber.

IS-41-style systems support roaming subscribers by transporting SSD from the HLR to the VLR. Knowledge of SSD enables the VLR to perform autonomous authentication of the user because the challenges and responses can be derived locally. This eliminates the need for additional HLR/VLR communications to provide further security information when needed. In addition, the visited system may utilize a "global" random challenge that can be broadcast on a system-wide information channel. The use of a global challenge enables the handset to respond to the challenge as a component of the service access request, thereby making efficient usage of bandlimited PCS channels.

An unauthorized interception of SSD upon transport to the VLR could result in a long-term impersonation of a user. IS-41-style systems employ a "Call Count" for protection from both this event and from general handset duplication, or "cloning." The call count is incremented in the handset upon a command from the network, generally during a call. The network also maintains the count. Later, during a subsequent access attempt, the handset sends its call count back to the network. If multiple handsets are sharing an identity, the network will accumulate a count that will likely exceed that of the legitimate user. Once a clone is suspected, network personnel can intervene. The preferred method of eliminating a clone is to request that the home network initiate the protocol to change the handset's SSD, as described above.

## Authentication and Key Agreement Protocol in Secret Key Systems

Figure 4 illustrates simplified call flow models for AKA in GSM-based systems (upper portion) and in IS-41-based systems (lower portion). In either case, the goals are to assure the serving network that the handset is entitled to service and to develop a set of cipher bits for protection of user traffic over the RF link.

GSM-based AKA utilizes a challenge/response protocol to perform authentication and to generate cipher bits. This protocol is executed at the discretion of the serving network; a typical occurrence would be during a call setup. The network begins the procedure by either generating or selecting a challenge/response pair, called RAND/SRES, respectively. If the handset is being served by its "home" network, the 128-bit RAND is generated locally and then combined with the user's Ki to form the 32-bit SRES. RAND is then sent to the handset, where the handset will combine RAND with Ki to produce SRES. SRES will be returned to the network for comparison with the SRES that was calculated internally. If the two match, the handset will be considered to be authentic. Additional processing on RAND and Ki will produce the cipher bits called "Kc." This will occur at both the handset and the network; Kc can then be applied at both ends to protect traffic. In GSM, the computational algorithms that are used to combine RAND and Ki are selected by the home service provider and need not be common throughout the system.

In a roaming situation, the above scenario is unchanged, except that the RAND/SRES/Kc triplets are precomputed by the home network.

Triplets are transferred to the visited network to support a roaming user as a result of handset registration and/or a request for additional security information. The VLR performs the SRES comparison and provides Kc to the encipherment function, based on inputs from the home network.

IS-41-based systems also utilize a challenge/response method to perform authentication and derive cipher bits. As discussed in the previous section, the user's security variable is SSD; this is intended to be passed from a home network to a visited network upon registrations. Hence, the challenge/response mechanism is identical for both home users as well as roaming users.

In an IS-41-style network, a single 32-bit "global" challenge is generated at frequent intervals and broadcast throughout the service area on a system information channel. Handsets that attempt a system access will compute an 18-bit authentication response by means of an authentication algorithm operating on their individual SSDs and the current global challenge. The access request package concatenates the registration/call setup information with the user's authentication response and call count value. For a registration, the response (and challenge) are sent to the home network for verification. If the handset is found to be authentic, SSD will be transported to the serving network along with other pertinent user data. During a call setup, receipt of the user's identity triggers a local data base lookup at the serving network to retrieve his SSD and call count. The authentication response is then verified when the serving network confirms that the retrieved SSD/global challenge combination can be applied to the authentication algorithm to produce the same response as that received from the handset. In addition, the call count is checked for accuracy. Further processing of the SSD/global challenge at both the handset and the local network then produces cipher bits for the protection of user traffic.

## User Confidentiality in Secret Key Systems

Both secret key methods provide a means for user authentication and subsequent protection of user traffic. However, the registration and/or call setup process must include an identification of the user in order that the network may retrieve unique security information assigned to the subscriber. A subscriber ID that is available over the airwaves may be a security risk, especially in low-mobility settings, because it reveals knowledge of a subscriber's location.

GSM systems have dealt with this problem by the practice of using "temporary mobile station identities" (tmsi). This scheme requires that a subscriber reveal his true identity upon initial access. During the first call, the network then assigns to him, under encryption, an identity that is only known to him and to the serving network. "tmsi" may be reassigned by the serving network at its discretion. Anonymous roaming is accommodated when the user sends tmsi and the ID of the (previous) serving network to the current network. The use of a clear subscriber ID is permitted during network failures.

IS-41-based systems, such as the "PACS" air interface, are adopting similar schemes for the protection of user identities.

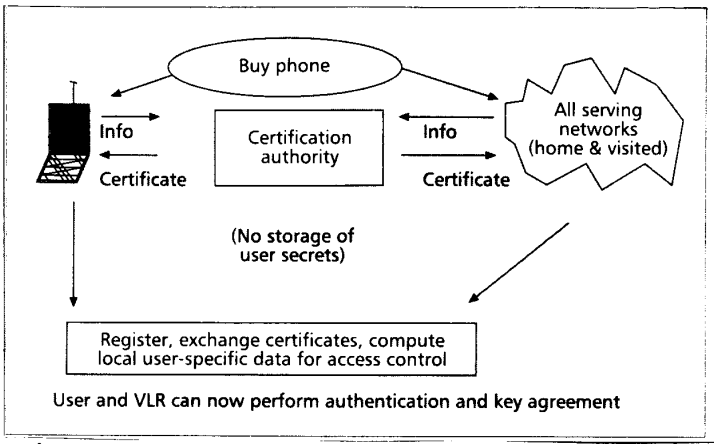


**Figure 5.** *Provisioning and roaming support: Public Key/Secret Key hybrid.*

## Introduction of Public Key AKA into PCS

PCS networks that emerge at 1.8 GHz are expected to adopt P&A techniques that are derived from some combination of existing GSM and/or IS-41 standards. However, additional security benefits may be realized by the introduction of public key techniques. The "PACS" air interface has already been designed with the capability of supporting a migration to a public key AKA method.

Public Key first appeared in mathematics journals in the mid-'70s, but has not been widely adopted for use in wireless systems. This is because most implementations required both excessive computations and the time-consuming transfer of large bit fields across noisy, bandlimited channels. However, three factors have enhanced the desirability of Public Key for PCS applications. First, some PCS air interfaces offer increased bandwidths over conventional cellular and two-way radio systems. Also, a low-mobility environment decreases the effects of channel fading. These considerations enable a quicker, more error-free transfer of large public key bit fields across a PCS channel. Second, the computational ability of low-cost processors continues to increase, which makes public-key mathematics less formidable. Third, recent studies [2] have proposed techniques that split the computational load unevenly between the PCS infrastructure and the handset. This enables the handset to perform relatively simple calculations, while the land-based infrastructure performs the intensive calculations.

The proposed public key method is summarized in Fig. 5, where the steps of provisioning and roaming support are combined for clarity. Once the access control information has been established, the AKA protocol for call setups can be performed using a secret key method, as in GSM or IS-41-based networks. This technique is referred to as the "Public Key/Secret Key Hybrid."

Handset provisioning begins when the user purchases a phone and requests service, as in the

*As of the last quarter of 1994, seven air interfaces were under development by PCS standards bodies: PACS, DCS, IS-136-based, IS-95-based, the composite CDMA/TDMA/FDMA system, wideband CDMA, and the DECT-based proposal.*

secret key case. The user will then approach a "Certification Authority" (CA) with his credentials and some identity information about his handset and/or SIM-like detachable User Identity Module. The CA will verify the accuracy of the information and "sign" a coded version of this information. The digital signature uses the private portion of the CA's public key pair; this signature is returned to the user as a "certificate." Any PCS network may check the validity of the certificate by applying the public portion of the CA's public key pair.

In a similar manner, the CA issues certificates to all PCS network Access Controllers after verifying essential information. This permits the subsequent validity check of a network by the handset, by applying the CA's public key as described above.

This simplified model of the public key method assumes that a single CA serves all PCS handsets and all PCS networks. It is possible to utilize multiple CAs in peer-to-peer or hierarchical arrangements, but this adds complexity. The goal is to use a minimum of CAs that are trusted by many service providers.

After the CA has issued a certificate to provision the handset, local security credentials are established with the serving network at the time of registration. These credentials are generated at the handset and sent to the serving network under public key encryption. This eliminates the need to send "triplets" or "SSD" via a network-to-network transfer.

A further application of public key in the hybrid protocol occurs when the handset performs a per-registration digital signature on access-specific information. This is done to prevent access through the use of stolen certificates.

An attractive feature of this hybrid method over secret key techniques is that all "private" keys are never distributed beyond their source. The CA signs certificates with its private key but distributes its public key for certificate validation. The Access Controller generates a private key for usage during a portion of the protocol, but broadcasts its public key for handsets to perform encryption. The handset generates a private key for use in its digital signature calculations, but sends its public key to the network for digital signature validation. The practice of not distributing a private key means that network "hackers" will not be able to infiltrate a data base of handset secret numbers at the network.

The hybrid method offers some protocol advantages as well. Since the Access Controller's public key is broadcast, a registration can be anonymous. This eliminates the need for network management of user confidentiality, as through a "tmsi" method. Also, there should never be a requirement that a clear ID be sent due to administrative difficulties.

A further benefit of the hybrid method is that the serving network establishes security credentials for the handset upon registration, instead of though an information transfer from the home network. The registration process involves a mutual validity check by both the handset and the network, based upon credentials that have been prevalidated by the Certification Authority. This reassignment of the source of trust enables a savings in network resources, since neither "triplets" nor "SSD" are required to be sent to a visited network to support a roaming user. However, it will still be necessary that the user's service profile and credit status be maintained at his home network and be available to visited networks in order to provide continuous service.

## Security Mechanisms of Proposed PCS Air Interfaces

As of the last quarter of 1994, seven air interfaces were under development by PCS standards bodies: PACS, PCS-1900, IS-136-based, IS-95-based, the composite CDMA/TDMA/FDMA system, wideband CDMA, and the DECT-based proposal. PACS security uses an IS-41-like AKA technique with the ability to migrate to the hybrid public key method. PCS-1900 uses a GSM-like security process. The composite system supports both GSM and IS-41 methods. Wideband CDMA, IS-136-based, and IS-95-based air interfaces rely on the IS-41-style P&A method. Various options remain under consideration for other air interfaces.

### References


[1] M. J. Beller, L. Chang, and Y. Yacobi, "Privacy and Authentication on a Portable Communications System," *Proc. IEEE Global Telecommun. Conf.*, Dec. 2-5, 1991, pp. 1922-1927.

[2] M. J. Beller and Y. Yacobi, "Fully-Fledged Two-Way Public Key Authentication and Key Agreement for Low-Cost Terminals," *Electronic Letters*, 27th May 1993, vol. 29, no. 11, pp. 999-1001.

[3] European Telecommunications Standards Institute (ETSI), "European Digital Cellular Telecommunications System (phase 1); Recommendation GSM 03.20, Security Related Network Functions, version 3.3.3, Jan. 1991.

[4] Electronic Industries Association, EIA Interim Standard IS-54, Rev B, "Dual-Mode Mobile Station-Base Station Compatibility Standard," 1992.


### Biography


DAN BROWN is a principal staff engineer in the Corporate Systems Research Labs at Motorola, Inc. Since joining Motorola in 1970, he has been involved in the development of commercial secure equipment. Recent activities include studies of authentication and voice privacy techniques for cellular phones and personal communications systems. He holds B.S.E.E. and M.S.E.E. degrees from the University of Illinois at Chicago.