

EXHIBIT 16

2

SERIAL NUMBER 07/378721		PATENT DATE		PATENT NUMBER	
SERIAL NUMBER 07/378721	FILING DATE 07/12/89	CLASS 340	SUBCLASS 925.340	GROUP ART UNIT 264	EXAMINER <i>H. H. ...</i>

APPLICANTS: MARY B. FLANDERS, WOOD DALE, IL; LARRY C. PUHL, SLEEPY HOLLOW, IL.

CONTINUING DATA**
 VERIFIED
 none PW

FOREIGN/PCT APPLICATIONS**
 VERIFIED
 none PW

FOREIGN FILING LICENSE GRANTED 09/06/89

Foreign priority claimed 35 USC 119 conditions met	<input type="checkbox"/> yes <input checked="" type="checkbox"/> no	AS FILED	STATE OR COUNTRY IL	SHEETS DRWGS. 3	TOTAL CLAIMS 15	INDEP. CLAIMS 6	FILING FEE RECEIVED \$ 718.00	ATTORNEY'S DOCKET NO. CEC2026R
---	--	----------	------------------------	--------------------	--------------------	--------------------	----------------------------------	-----------------------------------

Verified and Acknowledged
 Examiner's Initials: *PW*
 DONALD B. SOUTHARD
 MOTOROLA, INC.
 1303 EAST ALGONQUIN RD.
 SCHAUMBURG, IL 60196

TITLE: METHOD FOR AUTHENTICATION AND PROTECTION OF SUBSCRIBERS IN TELECOMMUNICATION SYSTEMS

U.S. DEPT. of COMM.-Pat. & TM Office -- PTO-436L (rev. 10-7)

PARTS OF APPLICATION FILED SEPARATELY

NOTICE OF ALLOWANCE MAILED		PREPARED FOR ISSUE		CLAIMS ALLOWED	
		Assistant Examiner	Docket Clerk	Total Claims	Print Claim
ISSUE FEE		Primary Examiner		DRAWING	
Amount Due	Date Paid			Sheets Drwg.	Figs. Drwg.
Label Area		ISSUE CLASSIFICATION		ISSUE BATCH NUMBER	
		Class	Subclass		
<p>WARNING: The information disclosed herein may be restricted. Unauthorized disclosure may be prohibited by the United States Code Title 35, Sections 122, 181 and 368. Possession outside the U.S. Patent & Trademark Office is restricted to authorized employees and contractors only.</p>					

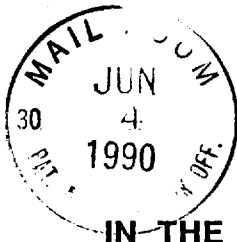
CLAIMS

What we claim is:

prote...

5
[Signature]

1. A method for facilitating communications between a first communication unit and a second communication unit, comprising the steps of:
- 10 A) providing the first communication unit with at least one ID and data to be transmitted;
 - B) providing the second communication unit with information regarding the ID;
 - 15 C) in the first communication unit, modifying the ID at least in part as a function of at least part of the data to be transmitted to provide a modified ID;
 - D) transmitting, from the first communication unit to the second communication unit, at least the modified ID and at least part of the data to be transmitted.



PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS:	FLANDERS ET AL.	EXAMINER:	WEISSMAN, P.
SERIAL NO.:	07/378,721	GROUP:	264
FILED:	JULY 12, 1989	CASE NO.:	CE02026R
ENTITLED:	METHOD FOR AUTHENTICATION AND PROTECTION OF SUBSCRIBERS IN TELECOMMUNICATION SYSTEMS		

Motorola, Inc.
Corporate Offices
1303 E. Algonquin Road
Schaumburg, IL 60196
May 30, 1990

AMENDMENT UNDER 37 CFR 1.115

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

Sir:

Responsive to the Office Action dated February 14, 1990, as entered in the above-captioned matter, the applicant hereby respectfully submits the following amendment and response.

In The Specification:

1. On page 1, line 26, please delete the words "network communication unit has access to these identification", as this line is a duplicate of line 1 on page 2.
2. On page 7, lines 19-20, please delete reference number "(28)" and substitute therefore reference number --(18)--; please delete reference number "(27)" and substitute therefore reference number --(19)--; and please delete reference number "(26)" and substitute therefore reference number --(17)--.

28-1

In the Claims:

Please amend claim 1 to read as follows:

1. (Once Amended) A method of authentication and protection as between a subscriber unit and a second communication unit in a radiotelephone communication system [for facilitating communications between a first communication unit and a second communication unit], comprising the steps of:
- A) providing the subscriber [first communication] unit with at least one ID and data uniquely identifying one of a plurality of target communication units to be transmitted;
 - B) providing the second communication unit with information regarding the ID;
 - C) in the subscriber [first communication] unit, modifying the ID at least in part as a function of at least part of the data to be transmitted to provide a modified ID;
 - D) transmitting, from the subscriber [first communication] unit to the second communication unit, at least the modified ID and at least part of the data to be transmitted.

Please amend claim 2 to read as follows:

2. (Once Amended) A method of authentication and protection as between a subscriber unit and a second communication unit in a radiotelephone communication system [for facilitating communications between a first communication unit and a second communication unit], comprising the steps of:
- A) providing the subscriber [first communication] unit with at least a first and second ID and data uniquely identifying one of a plurality of target communication units to be transmitted;
 - B) providing the second communication unit with information regarding the first and second ID;
 - C) in the subscriber [first communication] unit, modifying the first ID as a function of at least part of the data to be transmitted and the second ID to provide a modified first ID;
 - D) transmitting, from the subscriber [first communication] unit to the second communication unit, at least the modified first ID and at least part of the data to be transmitted.

Please delete claim 3 without prejudice.

2
29

Please amend claim 4 to read as follows:

4. (Once Amended) The method of claim 1 or 2 wherein the data to be transmitted includes at least identifying information uniquely identifying a requested [regarding a] third communication unit.

Please amend claim 6 to read as follows:

6. (Once Amended) A method of authentication and protection as between a subscriber unit and a second communication unit in a radiotelephone communication system [for facilitating communications between a first communication unit and a second communication unit], comprising the steps of:

- A) maintaining an historic non-arbitrary value in both the subscriber unit [first] and second communication unit[s], of predetermined communication events as between the subscriber unit [first] and second communication unit[s];
- B) transmitting, at least from time to time, from the first communication unit to the second communication unit, the historic non-arbitrary value [count] information as maintained by the subscriber [first communication] unit;
- C) receiving, at the second communication unit, the historic non-arbitrary value information;
- D) comparing, at the second communication unit, the historic non-arbitrary value information as received from the subscriber [first communication] unit with the historic non-arbitrary value [count] information as maintained by the second communication unit;
- E) when the historic non-arbitrary value information as received from the subscriber [first communication] unit is substantially the same as the historic non-arbitrary value information as maintained by the second communication unit, granting communication between the subscriber unit and one of a plurality of target communication units [taking a first predetermined course of action];
- F) when the historic non-arbitrary value information as received from the subscriber [first communication] unit is substantially different from the historic non-arbitrary value information as maintained by the second communication unit, providing output indicating that a multiple user is attempting to access the radiotelephone communication system [taking a second predetermined course of action].

Please amend claim 11 to read as follows:

11. (Once Amended) A method of authentication and protection as between a subscriber unit and a second communication unit in a radiotelephone communication system [for facilitating communications between a first communication unit and a second communication unit], comprising the steps of:

- A) providing the subscriber [first communication] unit with at least one ID, data uniquely identifying one of a plurality of target communication units, and an historic non-arbitrary value to be transmitted;
- B) providing the second communication unit with information regarding the ID;
- C) in the subscriber [first communication] unit, modifying the ID and the historic non-arbitrary value at least in part as a function of at least part of the data to be transmitted to provide a modified ID and a modified historic non-arbitrary value;
- D) transmitting, from the subscriber [first communication] unit to the second communication unit, at least the modified ID, the modified historic non-arbitrary value, and at least part of the data to be transmitted.

Please amend claim 12 to read as follows:

12. (Once Amended) A method of authentication and protection as between a subscriber unit and a second communication unit in a radiotelephone communication system [for facilitating communications between a first communication unit and a second communication unit], comprising the steps of:

- A) providing the subscriber [first communication] unit with at least a first, a second ID, an historic non-arbitrary value, and data uniquely identifying one of a plurality of target communication units to be transmitted;
- B) providing the second communication unit with information regarding the first and second ID;
- C) in the subscriber [first communication] unit, modifying the first ID and the historic non-arbitrary value as a function of at least part of the data to be transmitted and the second ID to provide a modified first ID and a modified historic non-arbitrary value;
- D) transmitting, from the subscriber [first communication] unit to the second communication unit, at least the modified first ID, the modified historic non-arbitrary value, and at least part of the data to be transmitted.

Please delete without prejudice claim 13 and dependent claims 14 and 15.

Please add independent claim 16 to read as follows:

16. (New claim) A method of authentication and protection of a subscriber unit in a radiotelephone communication system comprising the steps of:

- A) maintaining a count, in both the subscriber unit and a second communication unit, of predetermined communication events as between the subscriber unit and the second communication unit;
- B) providing the subscriber unit with at least a first ID, a second ID, and data uniquely identifying one of a plurality of target communication units;
- C) providing the second communication unit with a copy of the first ID and second ID;
- D) in the subscriber unit, modifying the first ID as a function of at least part of the data to be transmitted and the second ID, to provide a modified first ID;
- E) transmitting, from the subscriber unit to the second communication unit, at least the modified first ID, the count, and at least part of the data to be transmitted;
- F) comparing, at the second communication unit, the count as received from the subscriber unit with count information as maintained by the second communication unit;
- G) when the count as received from the subscriber unit is substantially the same as the count as maintained by the second communication unit, granting communication between the subscriber unit and the target communication unit; and
- H) when the count as received from the subscriber unit is substantially different from the count as maintained by the second communication unit, providing output indicating that a multiple user is attempting to access the radiotelephone communication system.

In The Drawings:

Included are corrected formal drawings (figures 1-3) wherein the correction entailed correcting the typographical misspelling of the word "encipher" in Figure 3, element 44. No other corrections were made.

REMARKS

1. In the above captioned Office Action, the Examiner rejected claim 1 under 35 U.S.C. § 103 as being obvious in view of Twardowski (U.S. Patent No. 4,535,333). Claims 2-5 and claims 11-15 were rejected under 35 U.S.C. § 103 as being obvious in view of Atalla (U.S. Patent No. 4,315,101). Claims 6-10 were rejected as being obvious in view of Atalla as applied to claims 2-5 and 11-15 and in further view of Ano et al. (U.S. Patent No. 4,023,012). The specification was objected to on a formality for need of further clarification, and the drawings were objected to because of a typographical misspelling. The Examiner further pointed out the obligation under 37 C.F.R. § 1.56 to disclose the inventors and invention dates of those claims that were not commonly owned by the instant assignee at the time the invention was made. The rejections are traversed and reconsideration is hereby respectfully requested.

2. The specification has been objected to for further clarification of the words "the information" on page 7, line 20. The "information" referred to is a copy of the serial number (18), the PIN (19), and the subscriber telephone number (17), which is information known to both the database and the subscriber unit. In the preferred embodiment, this information is a stored copy of the serial number, PIN, and the subscriber telephone as stated on page 7, lines 21-24. The specification has been amended to change the reference numbers as printed above to clarify the term "information" on page 7, line 20. However, those skilled in the art will recognize that other information known to both the subscriber unit and the fixed communication network may also be suitable.

3. The applicants wish to point out the field of invention of the claimed subject matter as being most particularly related to cellular-type radio frequency telecommunication systems. The amended claims reflect this limitation. The applicants believe it may be helpful to first characterize the Twardowski reference before discussing the merits of the Examiner's rejections regarding Twardowski.

THE TWARDOWSKI REFERENCE

The Twardowski reference discloses an apparatus for automatically and remotely modifying an identification code used between a receiver and transmitter.

When a different identification code is needed, the receiver generates a new random code from the old random code using a random number generator program. The receiver stores this new random identification code and then transmits it to the transmitter, which receives and stores the new random identifier. When communication is desired, the transmitter then communicates the new random identifier to the receiver. The receiver compares the identification code received from the transmitter to its stored version of the new random identifier to see if there is a valid match. If a match occurs, communication over a particular communication channel (as identified by the channel ID) is established. The format of the random code includes "data blocks and comprise four words each of four bits containing binary-coded information that can represent the code for a particular channel". (Column 3 lines 61-64). Therefore, Twardowski teaches randomly generating a new identification code at one unit and communicating this code to a second unit, wherein the new identification code (in the form of "data blocks") is stored and used as the proper identifier until another new random identification code is received, wherein it then becomes the proper identifier.

4. Claim 1 has been rejected under 35 U.S.C. § 103 in view of Twardowski. Claim 1 as amended is patentably distinct over Twardowski for several reasons. First, Twardowski does not teach or suggest modifying (encrypting) an identification number (ID) that distinguishes one subscriber from all others such as a personal identification number (PIN). Secondly, and more importantly, Twardowski teaches using a random number as an identifier and does not teach or suggest using a modified ID whereby the modified ID is modified using data that uniquely identifies one of a plurality of target communication units as now claimed by the applicants.

As disclosed in the best mode of operation, this data is the telephone number of the destination unit with which the subscriber wishes to communicate (page 8, line 1). Therefore, the data used to modify the one ID, as claimed by the applicants, is the unique telephone number of another cellular subscriber or landline telephone (target communication unit or requested communication resource), and is different for each telephone. This data uniquely identifies one of a plurality of possible destination units (each telephone being a possible destination unit) and is unique for each transaction. This type of data serves as a pseudo-random encryption key since no two telephones have the same telephone number, thereby affording sufficient protection against

eavesdroppers. In addition, the data as claimed by applicants is used for post-authentication activities.

The random identification code of Twardowski serves as an initialization identifier wherein no additional information is extracted or decoded from the random identifier to be later used for post-authentication activity. Although "other forms of digital information" (Twardowski, column 3, lines 61-64) may be inserted into excess bandwidth used for the random identification code, the code itself contains no information usable after authentication is granted.

As originally claimed by the applicants, "modifying the ID at least in part as a function of at least part of the data to be transmitted" (page 12, lines 13-15) makes "efficient use of of the data transmitted" (page 5, line 32) by using it as part of the cipher for enciphering the unique ID (PIN). The data referred to in applicants' amended claim 1 is information that is useful and necessary after authentication is granted to continue the transaction for which authentication was initially requested. Unlike the identification code in Twardowski, the ID of the applicants' invention is not a random number, nor is the data used to generate the modified ID a random number.

The utility of the data in the applicants' invention also effects the success of the completed call which is a post-authentication step unlike the limited usefulness of the random identification code suggested by Twardowski. The data is information used to effectuate proper routing of the call to a third communication unit (such as another remote subscriber unit). Consequently, both adequate ID security and efficient communication is facilitated by enciphering the ID using data unique to a destination communication resource. Claim 1 as amended more clearly states this non-obvious and novel distinction by requiring the data to uniquely identify one of a plurality of target communication units.

Furthermore, as stated by the Examiner, the "cooperative relationship between the data and the ultimate function to be performed is not critical to the Twardowski invention". A problem with which the applicants were faced, as stated on page 4, lines 5-19, concerned the need for an authentication and protection system that did "not require additional transmission processes or inject higher error levels during the authentication process". The Twardowski invention, however, performs its authentication using a random identifier code whose feature of randomness affords lesser probability of detection, but whose utility is limited solely to the verification of a proper random identifier code. Once verification is established, an output circuit is energized after which useable data may be communicated between the receiver and

transmitter. The random identifier does not contain useful post-identification data. Useful data must be sent separate from the random identifier.

The applicants' invention addressed this problem by modifying the ID as a function of the data and then communicates the modified ID with data to minimize the transmission processes. In a cellular telecommunication system, multiple subscribers are continuously vying for a limited number of communication channels, particularly during peak traffic times. A rapid access and reliable (secure) authentication process is paramount to minimizing base station and subscriber protocol overhead and authentication processing time. It also provides a subscriber unit quicker access to an available traffic channel. Twardowski does not teach or suggest that the random identification code is transaction-specific. If an eavesdropper reads the random identifier, he has complete communication access over the channel until the receiver is told to generate another random identification code. The applicants' method uses data specific to the transaction so that an eavesdropper detecting the modified ID may only communicate with the requested communication resource (the communication unit associated with the telephone number (data) used to modify the ID). Without the eavesdropper knowing the exact enciphering algorithm, the transmitted modified ID is unique for only one other target unit on the communication channel.

In addition, although the Examiner states that the Twardowski invention "can modify the ID for any common and suitable purpose, such as in relation to data", the applicants fail to find such a teaching in the Twardowski patent as no definition of data as claimed by the applicants can be found. Applicants claim that the data uniquely identifies a requested communication resource. Twardowski does not teach or suggest modifying the ID as a function of data. Therefore, the applicants respectfully submit that claim 1 be passed to allowance.

5. Independent claims 2, 11-13 and dependent claims 3, 4, 5, 14, and 15 were rejected as being unpatentable over Atalla. The Atalla reference was briefly described in reference to Figure 1A by the Examiner. As stated by the Examiner on page 4 of the Office Action, noting Figure 1A; column 2, lines 25-40; column 3, lines 45-70; and claims 1 and 2,

Atalla discloses a method and apparatus for securing data transmissions in which a PIN is provided. An ID code is generated at a first communication unit, in response to a PIN number that is entered and a random number (RN) that is generated. The RN and ID are both

transmitted by the transmitter 23 to the receiver 25, and the receiver compares the received ID (that was generated from the input PIN and the RN). This process is employed in order to permit conventional changes without compromising the security of data transfers or of identifying codes.

6. For Claim 2, the Examiner states that "the PIN and RN are the data to be transmitted that comprise the basis for the modification of the ID". Again, data, as described by the applicant on page 8, line 36, and page 9, line 1 (also page 6, line 24), is the dialed telephone number corresponding to a desired destination unit, and therefore uniquely identifies one of a plurality of requested communication resources and is also specific information necessary to complete the intended transaction. The random number (RN) in Atalla as referred to by the Examiner, is not data that uniquely identifies one of a plurality of target communication units as now claimed by the applicants.

As disclosed in the best mode of operation, this data is the telephone number of the destination unit with which the subscriber wishes to communicate (page 8, line 1). Therefore, the data used to modify the one ID, as claimed by the applicants, is the unique telephone number of another cellular subscriber or landline telephone (target communication unit or requested communication resource), and is different for each telephone. This data uniquely identifies one of a plurality of possible destination units (each telephone being a possible destination unit) and is unique for each transaction. This type of data serves as a pseudo-random encryption key since no two telephones have the same telephone number thereby affording sufficient protection against eavesdroppers. In addition, the data as claimed by applicants is used for post-authentication activities. Unlike the data as claimed by the applicants, the RN of Atalla is a merely a random number whose content is arbitrary and whose purpose is solely to enhance the degree of randomization in the encryption of the ID.

Also, the RN is not a second ID (as characterized by the Examiner). In Atalla, a new RN is generated for each authentication process regardless of what the PIN or account number of the user may be, whereas as known in the art, consistency and permanency is associated with an identifier so no two users ever have the same ID. When a random number is constantly generated and used as an identifier unique to a user, there is a chance that two users may wind up with the same random number.

The applicants wish to point out that Figure 1A, with respect to applicants' claim 2, is not as representative of applicants' claimed invention as is Figure 5A (from

Atalla), reproduced below for the Examiner's convenience, considering the number of ID's stated in the claim and the type of data referred to in the claim .

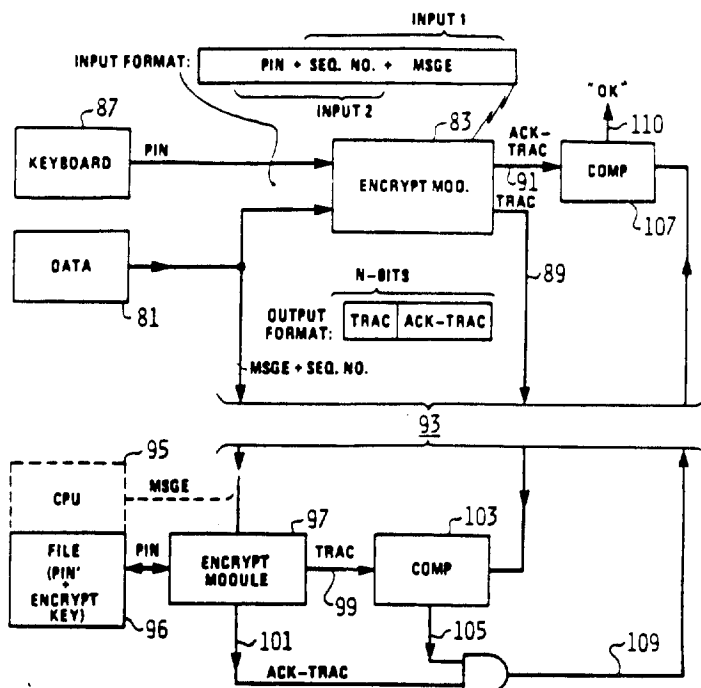


FIG. 5A

The applicants in original claim 2 claimed in part, "a first and second ID and data to be transmitted" and "modifying the first ID as a function of at least part of the data to be transmitted and the second ID to provide a modified first ID", and "transmitting at least the modified first ID and at least part of the data to be transmitted". As shown in Fig. 5A, the PIN 87 and data 81, not a random number (RN), are used in the encryption module 83 such that the input format to the encryption module includes the PIN 87 (i.e. applicants' second ID), a sequence number and a message field. As stated in column 6, lines 50-57, the data or message (MSGE) is that information, such as an account number (i.e. applicants' first ID) or amount of money being transferred, which is to be secured against alteration or unauthorized use whereas the sequence number may be the date and time of the transaction. The TRansfer Authorization Code (TRAC) (i.e. applicants' modified ID) is generated using the PIN and the sequence message and the MSGE.

Furthermore, the MSGE and the sequence number are shown to be communicated unencrypted over the communication link, while TRAC is the encrypted information. Atalla teaches that the message to be secured against alteration or detection is transmitted over the link without having been modified. In contrast, the data in applicants' invention is not the information sought to be secured, it is the first ID which is sought to be secured, therefore, it is modified using both data and a second ID (which does not get transmitted analogous to the PIN in Atalla) and then an encrypted first ID is transmitted over the communication link. Even if the PIN of Atalla is taken as analogous to the second ID and the MSGE of Atalla is taken to be analogous to the applicants' first ID and the sequence number of Atalla is taken to be analogous to applicants' data, Atalla teaches transmitting the first ID and the data in unencrypted form and also transmitting a modified ID (TRAC) as shown in Fig. 5A. The applicants' claimed invention teaches away from transmitting the MSGE in unencrypted form.

For the above-stated reasons, the applicants respectfully submit that claim 2 as amended be passed to allowance.

7. As to dependent claims 3-5, for the reasons stated above to allow claim 2 as amended, the applicants also respectfully submit that dependent claims 3-5 be passed to allowance.

8. Independent claims 11 and 12 are rejected since Atalla disclosed the subject matter as applied to claim 2 wherein the RN can be any suitable value such as an historic non-arbitrary value. The applicants respectfully dispute this characterization of Atalla for the reasons stated above (in section 6 of this amendment and response) and also dispute the characterization of claims 11 and 12. In Atalla, the RN is part of the encryption key for generating a modified ID, the historic non-arbitrary value (count) in claims 11 and 12 is not used as an encryption key. To the contrary, the historic non-arbitrary value is encrypted using the data as the encryption key. Furthermore, neither the RN of Figure 1A nor the sequence number, as stated above with reference to Figure 5A of Atalla, are encrypted before being transmitted as claimed by the applicants. These claims have been amended to include the clarifications as mentioned above with regard to amended claim 2. Therefore, the applicants respectfully submit that independent claims 11 and 12 as amended be passed to allowance.

9. Independent claim 13 is deleted.

10. Dependent claims 14 and 15 are deleted.

11. Independent claim 6 is rejected under 35 U.S.C. § 103 as being obvious in view of Atalla as applied to claims 1-5 and 11-15 and further in view of Ano et al. Applicants wish to point out a possible typographical error in the Office Action as Twardowski was the reference cited by the Examiner for claim 1, whereas Atalla is the cited reference for claims 2-5. It is applicants' belief that the words "Atalla as applied to claims 1-5 and 11-15" on pages 5 and 6 of the office Action should read "Atalla as applied to claims 2-5 and 11-15". Therefore, applicants will respond to the Office Action as though the Examiner intended to apply Atalla to claims 2-5 and not claims 1-5.

Examiner states that "Atalla discloses all of the subject matter claimed as applied to claims 2-5 [sic] and 11-15 except for the method of providing count information". Applicants respectfully dispute the Examiner's characterization of claim 6 as having any of the elements of claims 2-5. Applicants' claim 6 is directed toward the maintenance of a count of events as between a subscriber unit and a fixed network communication unit, and a comparison between the counts to determine whether a multiple user was attempting to access the system (as stated on page 5, lines 8-23 and on page 10, lines 24-27). Applicants' claims 2-5 do not contain the element of maintaining "predetermined communication events as between the first and second communication units" as claimed in claim 6 (page 15, lines 5-7).

As to the Atalla rejection, claims 13-15 are sought to be deleted and claims 11 and 12 amended for the reasons stated in sections 8, 9, and 10 of this response. Therefore, applicants will address the Examiner's rejection of claim 6 in view of Ano et al. The field of invention for Ano et al. is a card verification system as stated in column 1, lines 4-5 (also see claims 1, 9, 11, and 13) and not a cellular radio telephone communication system as claimed in amended claim 6.

As stated by the Examiner, Ano et al. "uses the balance of the users account for the purpose of checking the correctness of the secret number". However, applicants claim "an historic non-arbitrary value ... as between the first and second communication units". An account balance is arbitrary and may stay the same, regardless of the number of transactions initiated by the card user. For example, the user may deposit \$100.00 in the form of a check into a cash station machine and, during the same transaction, withdraw \$100.00 in the form of cash such that the

~~13~~

40

balance stays the same, thereby indicating no historic change due to the number of transactions. The account balance may not change even over a period of many transactions, in addition, automatic tellers tend to disperse money in increments of \$5 or \$10. An unauthorized user would have an easier time decoding the balance of a card user since the balance would change in these fixed increments. However, the telephone number as used in applicants' invention affords greater encryption protection since these numbers come from a much larger variable pool.

Furthermore, as stated by applicant on page 10, lines 24-27, the claimed invention detects multiple users employing the same serial numbers and telephone numbers (page 5, lines 24-26) such that unauthorized users may be detected and authorities may be notified "that a multiple user is attempting to access the system". Therefore, the system does not merely deny access to an unauthorized user (see Ano et al. column 7, lines 1-3), but an unauthorized user may be allowed access (or be fooled into thinking that the system is granting access) for a time long enough for authorities to detect the location of the thief. A second course of action referred to in claim 6, lines 25-26 has been amended to further clarify this distinction. Therefore, the applicants respectfully submit that independent claim 6 as amended be passed to allowance.

12. Claim 8 was also rejected under 35 U.S.C. § 103 as being obvious in view of Atalla as applied to claims 2-5 and 11-15 and further in view of Ano et al. As stated above, an account balance may stay the same for a multiple number of transactions resulting in an unauthorized user being allowed to use the same balance multiple times to gain access to the system. This is not an historic non-arbitrary value as claimed by the applicants.

In addition, claim 8 is dependent upon claim 6, which claim has been shown allowable above. Therefore, claim 8 constitutes patentable subject matter and the applicants respectfully submit that claim 8 is in proper condition for allowance.

13. Claim 7 was also rejected under 35 U.S.C. § 103 as being obvious in view of Atalla as applied to claims 2-5 and 11-15 and further in view of Ano et al. Claim 7 is dependent upon claim 6, which claim has been shown allowable above. Therefore, claim 7 constitutes patentable subject matter and the applicants respectfully submit that claim 7 is in proper condition for allowance.

14. Claim 9 was also rejected under 35 U.S.C. § 103 as being obvious in view of Atalla as applied to claims 2-5 and 11-15 and further in view of Ano et al. Claim 9 is dependent upon claim 6, which claim has been shown allowable above. Therefore, claim 9 constitutes patentable subject matter and the applicants respectfully submit that claim 9 is in proper condition for allowance.

15. Claim 10 was also rejected under 35 U.S.C. § 103 as being obvious in view of Atalla as applied to claims 2-5 and 11-15 and further in view of Ano et al. Claim 10 is dependent upon claim 6, which claim has been shown allowable above. Therefore, claim 10 constitutes patentable subject matter and the applicants respectfully submit that claim 10 is in proper condition for allowance.

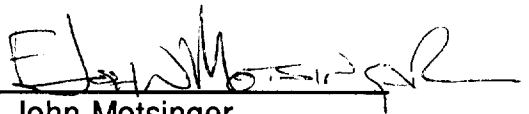
16. Claim 16 is an additional claim believed to be allowable in view of the prior art cited by the Examiner for the reasons stated in this response.

17. Applicants acknowledge the duty under 37 C.F.R. § 1.56 to inform the Examiner as to claims of inventions not commonly owned by the assignee at the time of invention. Applicants have also attached with this response a supplemental information disclosure statement including an application for patent owned by instant assignee and having as inventor Zdunek et al., filed April 04, 1988. The instant invention and the Zdunek et al. invention were commonly owned by the instant assignee at the time of invention by applicants.

19. The Examiner is invited to contact the undersigned by telephone or facsimile if the Examiner believes that such a communication may advance the prosecution of the present application.

Respectfully submitted,

FLANDERS ET AL.

By 
F John Motsinger
Attorney for Applicants
Registration No. 30,785
Phone: (708) 576-5213
Fax: (708) 576-3750

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, D.C. 20231, on 5/30/90
(Date of Deposit)
Flanders et al.
Name of applicant, assignee, or Registered Rep.
Jenny Hornik 5/30/90
Signature Date