25
4/3/79

SAND79-0070
Unlimited Release

MASTER

Secure Stand Alone Positive Personnel Identity Verification System (SSA-PPIV)

Paul D. Merillat

SF 2900 Q(7-73)

SAND79-0070
Unlimited Release
Printed March 1979

SECURE STAND ALONE

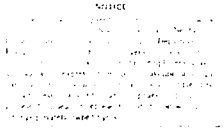
POSITIVE PERSONNEL IDENTITY VERIFICATION SYSTEM

(SSA-PPIV)

P. D. Merillat
Sandia Laboratories
Albuquerque, New Mexico 87185

Abstract

The properties of a secure stand-alone positive personnel identity verification system are detailed. The system is designed to operate without the aid of a central computing facility and the verification function is performed in the absence of security personnel. Security is primarily achieved by means of data encryption on a magnetic stripe badge. Several operational configurations are discussed. Advantages and disadvantages of this system compared to a central computer driven system are detailed.



Acknowledgements

The SSA-PPIV was designed and constructed under the guidance of Earle Chapman. The hardware was built and tested by Don Tipping. The software was designed by the author and implemented with the help of Larry Woellhart. Robert Lederer provided the algorithms for the data authentication techniques. To all these competent people the author expresses his sincere gratitude.

Table of Contents

List of Figures

SECURE STAND ALONE
POSITIVE PERSONNEL IDENTITY VERIFICATION
(SSA-PPIV)

Introduction

This report details the properties of a positive personnel identity verification (PPIV) device which was constructed as an optional domestic feature of an international nuclear material containment portal. SSA-PPIV consists of a unit which verifies the identity of a user and another, separate unit which enrolls the user into the system. The verification unit is designed to be operated in the absence of security personnel and without the need of a central computing facility.

OVERALL DESCRIPTION:

The SSA-PPIV was designed as an optional domestic feature for an international nuclear material containment portal. This portal is a unit which denies passage to a user suspected of having nuclear material on his person. The SSA-PPIV unit adds the domestic capability of ascertaining that the user has obtained authorization to enter a controlled area. This is done by comparing a measurement of a person's physical features with stored data specifying those features. This comparison determines that a user is who he claims to be.

The design constraints of the international portal suggest certain design features of the SSA-PPIV. The international portal is fully automated to the extent that full time human supervision is not required for normal operation. For compatibility, the SSA-PPIV should be usable in this fashion as well. The nuclear material containment portal operates without

benefit of a central computing facility so the SSA-PPIV should be independent as well. The SSA-PPIV may, however, utilize existing capabilities of the international portal's microprocessor.

The operational control of the containment portal will be with an international inspector. For a PPIV system to be useful, the administrative control of its operation must be local. This implies that the SSA-PPIV unit must be designed in such a way that it does not adversely impact the international operation while allowing operational control to be effected at the local level.

With these constraints in mind the following SSA-PPIV system was defined. The physical feature chosen for identification comparison was hand geometry. The Identimat Corporation markets a microprocessor controlled hand scanner which compares a subject's hand geometry with stored hand geometry data. This off-the-shelf unit was modified with a non-metallic faceplate to minimize interference with the international portal's metal detector. This modification is not required if the SSA-PPIV is not associated with a metal detector. To make it more difficult for more than one subject to attempt entry with a single credential, the subject's weight is stored and compared with a weight reading taken at the time of use. For added security, a user is required to enter a five-digit memorized code with each entry attempt. This weight and code data is stored along with the hand geometry data. Since no central computing facility is available, storing the comparison data in a secure fashion becomes important. The data is stored on a badge with a magnetic stripe on it. Note that it is not sufficient to store this data in a manner that can be easily understood since if it were, forged badges would be relatively easy to make. For this reason the data on the badge is

encrypted using a sophisticated encryption algorithm. It is still possible to copy a badge but an adversary must also duplicate the hand geometry, weight, and memorized code to gain access.

The above design features are mandated by the constraints itemized previously. There are some additional features which were incorporated to make the device more versatile. Each SSA-PPIV in a given installation is assigned an area number so that users may be allowed through only those units authorized at enrollment time. The SSA-PPIV is made aware of the date and time so that certain users may be granted access only for a specified period of time. This is useful for visitors and short-term employees. In the case of lost badges or terminated employees, it is possible to block any badge which has been issued by informing the SSA-PPIV of the ID numbers of badges which are blocked. An issue level is associated with each badge allowing an installation to void an entire series of badges and re-enroll all authorized personnel. The SSA-PPIV controller, which is a microprocessor, also keeps track of who is currently inside a controlled area. Providing the verification unit controls entry to an area with only one normal entry point, this allows enforcement of the two man rule as well as preventing unauthorized passage by a person passing his badge and hand geometry template back for an adversary to use.

Local control of the SSA-PPIV is effected by authorized facility staff initializing the SSA-PPIV unit when it is powered up. The initialization data consists of date, time, level of issue, area designation and a list of those ID's which are blocked from the system. This is done by hand since there is no central computing facility which can do automatic initialization.

An identity check is requested of the SSA-PPIV by the international portal microprocessor via a serial communications link. The result of the check is sent back to the international controller and the international controller will write this result on its own log tape. This log tape can be made available to the installation for its records and security functions. It is also possible for the installation to monitor the output to the log tape so that it may receive immediate indications of possible abnormal usages.

ENROLLMENT STATION:

The enrollment station is part of the SSA-PPIV system. Its function is to produce badges for authorized employees and to keep a record of all enrollments. It is totally separate from the verification unit. A block diagram of the enrollment station appears in Figure 1.

The major components of the enrollment station are:

1. A Texas Instruments input/output terminal with hard copy and cassette tape drive. This is used to communicate with the enroller and to keep a permanent record of enrollments on the cassette tape.

2. An Identimat Corp. hand geometry scanner. This is used to obtain the enrollee's hand geometry data.

3. An Elcom Industries badge encoder. This is used to write the encrypted data on the badge.

4. A Harco Industries badge reader. This is used to verify that the data has been correctly written on the badge.

5. A Motorola microprocessor system. This controls the enrollment and encrypts the data to be written on the badge.

6. A Detecto Scales, Inc., weight scale. This is used to obtain the enrollee's weight.

The enrollment procedure consists of the following steps:

1. The operator weighs the enrollee.

2. The operator, on request of the enrollment microprocessor, enters the enrollee's name, ID number, weight, expiration date, issue level and areas to which the enrollee has access.

3. Under control of the enrollment microprocessor, the enrollee uses the hand geometry scanner in enrollment mode. The scanner sends the hand geometry data to the enrollment controller.

4. The operator verifies the entered information and if correct indicates so to the system. The microprocessor writes the enrollment information on the cassette tape.

5. The enrollment microprocessor encrypts the data and writes it on the badge.

6. The controller informs the enrollee of his memorized code.

7. The operator by request of the controller runs the badge through the badge reader and the station verifies that it was correctly written. This completes enrollment. The enrollee may now gain access to specified areas under the enrollment constraints.

VERIFICATION UNIT:

The verification unit of the SSA-PPIV resides at the access point of the controlled area. Its function is to verify that the badge holder attempting to gain access is the owner of the badge and that this person is authorized to gain access to the controlled area based on those constraints specified at enrollment. A block diagram of the verification unit appears in Figure 2.

The major components of the verification unit are:

1. An Identimat Corp. hand geometry scanner. This is used to obtain a hand geometry reading of the user.

2. A Detecto Scales, Inc., weight scale. This is used to obtain a weight reading of the user.

3. A Harco Industries badge reader. This is used to obtain the comparison data from the user's badge.

4. A Motorola microprocessor system. This is used to control the verification system, to communicate with the international portal microprocessor and to decrypt the badge data.

5. An RCA micro-terminal. This is used to input the initialization data into the verification system.

When the system is powered up, a light on the SSA-PPIV display panel will indicate that the system requires initialization. Initialization is performed by plugging in the RCA micro-terminal and inputting the required data. The micro-terminal looks very much like a hand held calculator. The operator

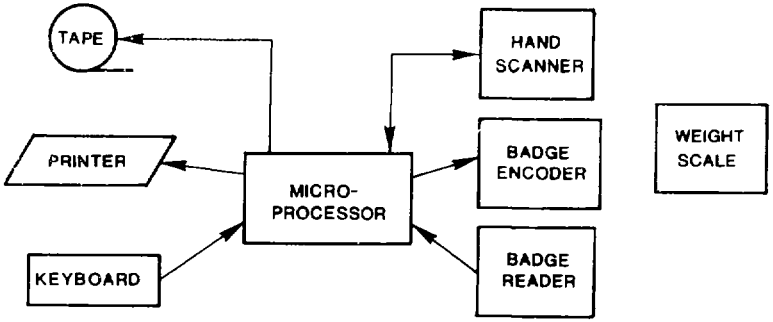


Figure 1. Enrollment Station Functional Diagram.

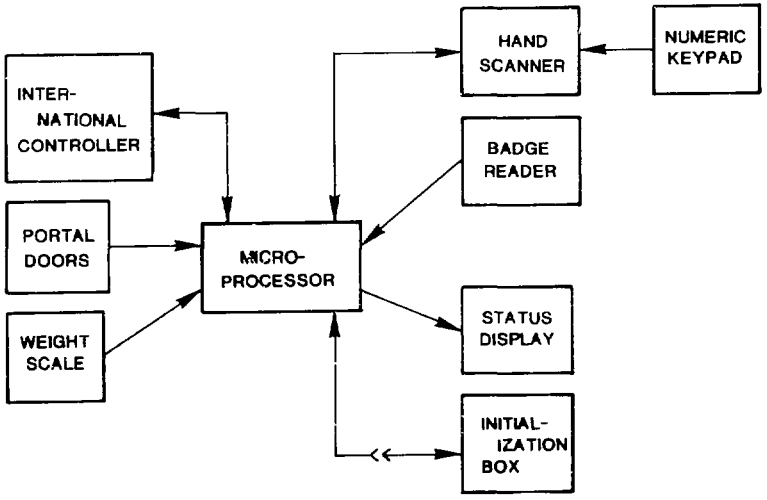


Figure 2. Verification Unit Functional Diagram.

identifies himself to the SSA-PPIV system via a five-digit memorized code. When verification is complete, the operator enters the date, time, level of badge issue, designated area and any badges blocked from the system. The operator may reinstate previously blocked badges and may also cause a list of initialization constraints to be displayed. Should a user attempt entry through a non-initialized system, the system will work normally with the exception that the entry will not be denied based on blocked badge, incorrect issue level, wrong area or expired badge.

Normal use of the verification unit is as follows:

1. The user enters the portal and the international controller issues a verification request to the SSA-PPIV. The SSA-PPIV lights an "INSERT BADGE" light.

2. The user draws his badge through the badge reader. He is allowed up to three tries.

3. The SSA-PPIV decrypts the badge and performs comparisons for weight, blocked badge, level of issue, area, expiration date and occupancy. If this is an exit request the check is finished. The user is always allowed to leave. Any discrepancies are noted in the result message returned to the international controller. If this is an entry request and there are any discrepancies, the user is denied access and the discrepancies are noted in the return message. Reasons for failure are displayed to the user on the SSA-PPIV display panel. These indications remain lit until the next verification request is received.

4. For entry requests which have not yet produced a discrepancy, the SSA-PPIV displays the "ENTER NUMBER" light.

5. The user enters his memorized five-digit number. An incorrect number terminates the check and will inhibit this badge from passing for three minutes to prevent an adversary from gaining access by repeatedly trying different numbers.

6. If the number is correct, the user is instructed to use the hand geometry scanner. He has up to three tries on each hand; either hand passing allows access.

7. The SSA-PPIV returns the result to the international processor. The international processor will allow or deny passage based on this result and its own checks. The result is written on the international log tape and is also available for immediate monitoring by the installation.

SECURITY AND DATA ENCRYPTION:

In a central computer controlled PPIV system, overall security is primarily a function of two things. The first is the security of the stored data and the second is the security of the communication link. In the case of the SSA-PPIV, the security rests primarily in the difficulty involved in forging a new badge, i.e., making a new badge which will pass the adversary through the SSA-PPIV. Note that the ability to duplicate a valid badge does not in itself pose a threat. If an adversary duplicates a badge, he must still use the hand geometry specified on the badge as well as the weight and memorized code.

The encryption algorithm used in the SSA-PPIV is a member of a class of relatively new encryption algorithms. Information on these algorithms has been published under "Public Key Cryptosystems," "Trapdoor Functions" and "Asymetric Cryptosystems."

The one being used for the SSA-PPIV was developed by Rivest [1] based on the difficulty of factoring very large numbers (on the order of 200 digits) into two prime factors. This system has two useful properties.

The first is the immense difficulty of breaking the cryptosystem. The Rivest cryptosystem bases its security on the difficulty of factoring large numbers. In their report on this cryptosystem, Rivest, Shamir and Adelman state that for a cryptosystem with a 100 digit key, 2.3×10^{23} operations are required to break the code [1]. At one million operations per second, 73 years of computation are required. Note that this assumed speed requires a special purpose device to be designed and built. Using current technology computers one expects an increase of a factor of at least 100 in the time to perform this task.

The second important feature of this cryptosystem is its asymetric implementation whereby one key is used to encrypt the data and another key is used to decrypt the data. It is not computationally feasible to calculate one key given the other. In the case of the SSA-PPIV, the encrypt key resides in the enrollment station and the decrypt key resides in the verification unit. This means that even if the decrypt key is extracted from the verification unit it is still not possible to forge a new badge. This requires the encrypt key. The implication of course is that the enrollment station must be secure but this must be done in any case otherwise an adversary could make a forged badge with the station. It is also worthy of note that if an adversary obtains a badge and knows what the data on the badge decrypts to, he still does not have enough information to produce badges of his own.

A detailed mathematical discussion of the cryptosystem is beyond the scope of this report. Details may be obtained from [1]. A less rigorous discussion of these algorithms appears in Martin Gardner's column in Scientific American [2] as well as the science section of Time magazine [3].

OTHER APPLICATIONS:

The SSA-PPIV is specifically designed to be an element of an international portal and as a result utilizes two features which exist in the containment portal's controller. The first feature is that of door control. The international controller listens for user requests via access buttons on either door and controls entry and exit via magnetic locks. The second feature is that of logging the results of checks and usages via its cassette log tape.

If the SSA-PPIV were to be used by itself, these features would have to be added. This primarily involves changes to the software. The operating system and control programs in the SSA-PPIV are purposefully modular to facilitate such changes. There are two primary configurations which would be relatively straightforward to implement.

The first is a single controlled door configuration. Here the SSA-PPIV would reside on the outside of the controlled area next to a controllable entry door. An entry request would be made via a request button located on the unit. Passage would procede as before. A successful check would cause the controllable door to be unlocked. An exit request would be made via an exit request button located on the inside of the controllable door. The door would automatically be unlocked and the user would then log out using his magnetic stripe badge. Note that in this configuration, a bad insider may let any number of adversaries pass along with him.

The second configuration would be a two door portal. The SSA-PPIV would be located inside with request buttons located on the outside of both doors. Operation would be identical to that of the containment portal with the exception that the PPIV check is all that is done.

The weight check is currently intended to verify that only one person is attempting passage. The tolerance for a correct weight check is therefore large (around 20 kg). If this philosophy is retained, it implies that the weight scale is not required for the single door configuration. If the tolerance is tightened, it can be used as an added verification check in which case it is appropriate to leave it in.

Use of the initialization unit currently requires the operator to identify himself via a five-digit memorized code. This requirement can be eliminated and the initialization device protected or the identification may be made more rigorous by requiring identification to be done via the hand geometry scanner.

Logging the results of a granted or denied passage could be done one of four ways. The first is no logging at all. Here the SSA-PPIV just grants or denies access. Secondly, results could be logged to a hard copy unit. This produces human readable but not machine readable logs. The third option is to write the log on magnetic tape. This would produce a machine readable log which could ultimately be used to produce usage and operational reports. The last option is to transmit the results to a computer giving the possibility of creating an on-line guard display. This might be appropriate if several SSA-PPIV units were installed at one facility. One can also consider a combination of the mentioned options.

TRADE-OFFS:

The primary advantage of the SSA-PPIV system over central computer driven systems is that of cost of purchase and installation. The SSA-PPIV system becomes feasible to those installations which do not have a central computing facility or to those whose central computing facilities do not lend themselves to the attachment of an on-line, real-time device. The installation is less expensive for several reasons. One is that there are no software costs associated with the central computer. Another is that the SSA-PPIV requires no communications links, secure or otherwise. The approximate costs would be:

Enrollment Station

Hand Geometry Scanner	$7,000
Operator Terminal (Tape, Hard Copy)	3,800
Badge Encoder	4,250
Badge Reader	1,000
Microprocessor System	1,500
Weight Scale	500
Housing	900
Badge Laminator and Accessories	2,000
	$20,950 + Labor

Verification Unit

Hand Geometry Scanner	$ 7,000
Badge Reader	1,000
Microprocessor System	1,500
Weight Scale	500
Housing	900
	$10,900 + Labor

The price of the housing for the verification unit will depend on the amount of physical security afforded by the housing and will be installation dependent.

Note that the above estimates do not include the cost of assembly or installation.

Two basic limitations are imposed by not having a central computing facility control the units. One is that it may not be appropriate to install the SSA-PPIV at the entry points to a controlled area which has more than one entry point, or at an installation whose throughput requirements would necessitate more than one unit. For these applications, it is not possible for the verification units to keep accurate occupancy lists. This prevents enforcement of the two man rule and also precludes denying entry to a user who is already inside as he may have left via the other unit. Not denying entry in this condition allows badge pass-back to work. That is, any number of adversaries could obtain entry by using a hand geometry template and memorized code of an insider by using the unit and passing the badge and template back to the next adversary. A multi-entry point configuration still provides reasonable security but is not as strong as the single entry point configuration.

The second limitation has to do with the hand geometry scanner. The Identimat supplied software in the scanner allows for the fact that human hand geometries change. This happens with fingernail growth, change of opacity of nail polish and the like. Also, as the user becomes familiar with the use of the scanner, his hand placement will become more uniform but may differ somewhat from the placement used at enrollment. To allow for this, when a user passes, the scanner returns updated hand geometry data which is intended to replace the old data. This works when the data is stored on a mass storage medium of a central computer. Since the SSA-PPIV has no such storage, this feature cannot be used. In order for this not to affect normal operation, the tolerance, or the error allowed during

comparison, is higher than it would be if data updating was possible. There are two types of errors associated with the hand geometry data comparison. Type I errors are those which deny a legitimate access request. Type II errors are those which pass an illegitimate access request. As the tolerance increases, Type I errors decrease but Type II errors increase. In the non-updating configuration the tolerance must be higher than in the updating configuration to keep the Type I error rate the same. This implies that in the non-updating configuration the Type II error rate will be higher. This higher error rate is compensated for by requiring the entry of the five-digit memorized code. If the tolerance is kept as low as in the updating configuration, more re-enrollments would be expected.

SUMMARY:

This paper has discussed the salient features of a secure stand alone positive personnel identity verification system. The device centers around hand geometry identification techniques coupled with the secure storing of the relevant data on a magentic stripe credential. The advantages and disadvantages of this system are compared to similar central computer controlled systems.

REFERENCES:

1. Rivest, Shamir, and Adelman, "A Method for Obtaining Digital Signature and Public-Key Cryptosystems" MIT/LCS/TM-82, MIT, Cambridge, MASS, April, 1977.

2. Gardner, Martin, "Mathematical Games" Scientific American, pp. 120-124, August, 1977.

3. Time Magazine, pp. 55-56, July 3, 1978

DISTRIBUTION:

U. S. Department of Energy
Office of Safeguards and Security
Washington, DC 20545
Attn: Burt Newmark, Chief
Physical Protection Branch

1700 W. C. Myre
1710 V. E. Blake
1730 C. H. Mauney
1750 J. E. Stiegler
1754 I. G. Waddoups
1757 V. K. Smith
1758 C. E. Olson
1759 M. J. Eaton
1759 E. R. Chapman
1759 D. L. Mangan
1759 P. D. Merillat (10)
1759 D. W. Tipping
1759 L. E. Woellhart
1760 J. Jacobs
1761 T. A. Sellers
3141 T. L. Werner (5)
3151 W. L. Garner (3)
for DOE/TIC (Unlimited Release)
3172-3 R. P. Campbell (25) for DOE/TIC
8266 E. A. Aas