



Biometric Authentication Credential in the Criminal Justice System





Center for
**Criminal
Justice
Technology**

MTR-2004-20

Mitretek Technical Report

Biometric Authentication Credential in the Criminal Justice System— Applications to Access Control

November 2004

Linda Jones Nichols, D.Sc.

Darric Milligan

Lawrence D. Nadel, Ph.D.

Eeshat Ansari

Thomas P. Murphy



**Supported under Cooperative Agreement 2001-LT-BX-K002
Office of Science and Technology
National Institute of Justice
Office of Justice Programs
U.S. Department of Justice**

Points of view in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Justice.

Mitretek strives to provide the latest and most complete information in its documents and makes such documents available for informational purposes only. You may not copy or otherwise use this document or its contents for commercial gain. Mitretek is not responsible for the uses you make of the information provided herein.

© Mitretek Systems 2004 All rights reserved



Innovative Technology in the Public Interest

3150 Fairview Park Drive South, Falls Church, VA. 22042

Executive Summary

Mitretek Systems is a nonprofit company, chartered in the public interest that provides research and engineering support to all levels of government. The Center for Criminal Justice Technology (CCJT) is a “center of excellence” that provides unbiased technology expertise to the criminal justice community. Mitretek Systems operates the CCJT and receives federal funding to partner with state and local agencies in developing adaptable approaches for modernizing systems and practices that improve the efficiency, safety, and coordination of criminal justice agencies. In coordination with the Office of Justice Programs, National Institute of Justice, Department of Justice, CCJT annually selects projects because of their national significance and because they are critical to state and local criminal justice agencies of all sizes.

This report summarizes the project entitled *Biometric Authentication Credential in the Criminal Justice System—Applications to Access Control* conducted by CCJT under the National Institute of Justice (NIJ) Cooperative Agreement 2001-LT-BX-K002.

Criminal justice operations rely greatly on the correct identification of individuals who pose threats to national and local security. These operations also rely on providing access only to those individuals who have been positively identified and authorized access to criminal justice system and related components. Positive identification of an individual can be no more effective than the up-front credentialing process – the individual is correctly identified and uniquely enrolled as one who has been approved for or is entitled to access. Biometric authentication credentialing is an approach that can enhance the processes of identification and access control. Biometrics are defined as physical or behavioral characteristics that can be measured and compared by automated means to determine or verify the identity of an individual. Credentialing is the process of compiling storing information about an individual on a card, device, or other personal medium that typically remains with the individual.

Access control is the fundamental application of biometric authentication credentialing that was explored in this project. Potential needs for officer and staff credentialing include controlling access to restricted or secure facilities or locations, controlling access to secure systems and information (e.g., maintaining critical infrastructure such as telecommunication facilities or computer data centers, submitting reports, accessing databases), and controlling access to services, equipment, or privileges. Operations within the criminal justice system, such as positively identifying visitors to prisons, individuals as they move about a prison—or between prison and courthouse, and individuals who are released from prison, can benefit from the implementation of biometric identification technology.

The agencies at the focus of this project are state, regional, and local criminal justice agencies since agencies at these levels are generally the first to initiate and provide criminal justice processing and services. Given the growing emphasis on Homeland Security, the need for secure and interoperable credentialing between criminal justice entities and first responder and public safety agencies has become apparent. The approach taken for this project was to first make initial determination of criminal justice entities and operations where positive identification of officers and staff is critical and where credentialing could improve both the conduct and security of operations. We then sought to partner with an agency that had needs that might be addressed by biometric authentication credentialing, had the ability and desire to help identify and evaluate their needs, and was willing to apply their professional expertise to the development and evaluation of a proof-of-concept. The Arlington County, VA Department of Public Safety and Emergency Management, Police Department (PD), and Office of the Sheriff were chosen. Next, basic concepts of operation for use of a biometric authentication credential were developed for law enforcement and corrections. Criminal justice operations with a potential need for access control using biometric authentication credentialing were further investigated and evaluated with regard to practicality, feasibility, and usefulness. Development of the basic concept into a hands-on proof of concept demonstration followed. The proof of concept demonstration was developed and tested at Mitretek prior to setup at Arlington County. The final step in the project was to develop guidance and a cost and benefit tool to help criminal justice technology officers assess the feasibility of an access control program using biometric authentication credentialing. The tool is an interactive Microsoft® Excel model that includes extensive information on potential weaknesses of identification technologies and presents various access control options. Qualitative and quantitative benefits are considered.

This project produced a number of conclusions regarding biometric based credentialing that can be grouped into the following five categories: biometric efficacy, requirements and standards, software development needed to support applications, costs versus benefits, implementation, and interoperability. There is potential for biometrics to improve security, as compared to manual access control options and as compared to access control options that are not uniquely linked to those who should be granted access. Requirements and standards for a biometric based credential are needed for planning and implementation within a single agency or program, as well as to ensure interoperability with other agencies or programs. Software development providing interfaces between an agency's or program's systems and databases is necessary to obtain the full benefit of biometric based access control systems. Costs and benefits associated with access control systems vary widely and may be quantitative, qualitative, or have likelihoods of low occurrence, making cost and benefit assessments difficult. Initial application of a biometric authentication credential should be to a well-defined system and a well-characterized population, where baseline cost and performance can be measured prior to integration into more complex operations.

Acknowledgments

Many individuals contributed to this project. First and foremost, the authors thank the Arlington County staff noted immediately below for their participation and support. They graciously devoted the time to share their professional expertise, offer and review new ideas, test and evaluate concepts, and review project deliverables.

Department of Technology Services

John Stevens (Program Manager, Public Safety and Emergency Management Technologies)

Police Department

Captain Dan Murray (Section Commander, Systems Management Division, Information and Technology Management Section)

Ann K. Mountjoy (Systems Management Division)

Lieutenant Paul Larson

Office of the Sheriff

Major Karen Albert (Director of Administration)

Captain Bill McKnight (Manager, Information Technology)

Phillip Chan (Technology Analyst)

Sergeant Terry Adams (Deputy Sheriff)

Sergeant Jimmy Barrett (Deputy Sheriff))

Deputy Phil Criss, (Deputy Sheriff)

Deputy Don Jones (Deputy Sheriff)

Office of Emergency Management, Emergency Communications Center

Lisa Thompson (Radio System Manager)

Fire Department

James Schwartz (Fire Chief)

Special thanks are extended to Dr. Allan Turner (U.S. Department of Homeland Security, Office of Domestic Preparedness and George Mason University) and Lt. Col. (Retired) Billy Dickson (Department of Homeland Security Consultant and Retired from Florida Department of Highway Safety and Motor Vehicles) for sharing their knowledge regarding local and national criminal justice programs. The authors also acknowledge Lolie Kull (Department of Homeland Security, Transportation Worker Identification Credential [TWIC] Program Manager) for providing information and insight regarding the planning and pilot implementation phases of the TWIC program.

The authors thank Sherrill Edwards (Mitrotek Systems) for her expert technical assistance in preparing this manuscript.

Trademarks

Microsoft® - Microsoft is a registered trademark of Microsoft Corporation

Windows® - Windows is a registered trademark of Microsoft Corporation

BPID™ - is a trademark of Privaris Corporation



Innovative Technology in the Public Interest

Table of Contents

1	Introduction.....	1-1
1.1	Background.....	1-1
1.2	Objectives and Scope.....	1-2
1.3	Approach.....	1-3
1.4	Organization of this Document.....	1-4
2	Biometric Credentialing Technology and Applicability to Access Control.....	2-1
2.1	Biometrics.....	2-1
2.2	Credentialing.....	2-2
2.3	Potential Applications of Biometrics and Credentialing in Law Enforcement and Corrections	2-5
2.4	Biometrics and Credentialing Programs	2-7
2.4.1	HSPD-12.....	2-8
2.4.2	DoD CAC.....	2-8
2.4.3	TSA TWIC.....	2-9
3	Biometric Credential Technology Applications.....	3-1
3.1	The Basic Concept.....	3-1
3.2	Application to Arlington County	3-3
3.2.1	Extensions of the Basic Concept to Daily Operations	3-3
3.2.2	Other Considerations	3-5
4	Proof of Concept Technology Evaluation and Demonstration	4-1
4.1	Technology Selection.....	4-2
4.1.1	Background.....	4-2
4.1.2	Fundamental Requirements	4-3
4.1.3	Description of the Selected Technology	4-4
4.2	Operational Demonstration of Biometric Authentication Credentialing Technology (Fingerprints)	4-7
4.2.1	Purpose.....	4-7
4.2.2	Approach.....	4-7
4.2.3	Results.....	4-8
4.3	Scenario Demonstrations	4-11
4.3.1	Creation of a Biometric Based Credential	4-12
4.3.2	Accessing a Secure Site	4-15
4.3.3	Officer Roll Call	4-17
4.3.4	Computer/Network Access	4-19
4.4	Results Summary	4-19

5	Costs and Benefits for Basic Concept	5-1
5.1	Approach.....	5-1
5.2	Model Assumptions	5-1
5.3	Model Description	5-2
5.3.1	Project Introduction and Model Information	5-2
5.3.2	Model Input.....	5-3
5.3.3	Results.....	5-7
5.3.4	Additional Considerations	5-7
5.4	Final Note.....	5-9
6	Conclusions.....	6-1
	References.....	RE-1
	Appendix A Biometrics and Corrections	A-1
	Appendix B Corrections Operations.....	B-1
	Appendix C Application of the Proof of Concept to the Inmate Population.....	C-1
	Appendix D Application of the Proof of Concept to Critical Incident Management.....	D-1
	Appendix E Proof of Concept Product Use Information	E-1
	Acronyms	AC-1

List of Figures

Figure 2-1	Operation of a General Biometric System	2-1
Figure 2-2	Applications of Personal Identification in Corrections and Law Enforcement.....	2-6
Figure 3-1	Biometric Authentication Credential (BAC) Concept.....	3-2
Figure 4-1	The Arlington County, VA Police Department, Courthouse, and Detention Facility are Collocated	4-1
Figure 4-2	Privaris BPID™	4-4
Figure 4-3	Privaris BPID™ LFBT Conceptual Diagram.....	4-5
Figure 4-4	Police Officer Authenticates the Privaris BPID™ Security Device Using His Left Thumb to Obtain Doorway Access	4-9
Figure 4-5	Illustration of Screen Sequence for Enrolling a Fingerprint Biometric.....	4-13
Figure 4-6	Data Entry for Credential Creation	4-14
Figure 4-7	Configuration of the Mobile Access Control Station	4-15
Figure 4-8	Illustration of Entry/Exit Workstation Screens.....	4-16
Figure 4-9	Illustration of Entry/Exit Log.....	4-17
Figure 4-10	Illustration of Officer Roll Call Data Capture Screen.	4-18
Figure 5-1	Map of the Model Screen.....	5-3
Figure 5-2	Background Program Information Data Entry Screen.....	5-4
Figure 5-3	Cost of Resources Data Entry Screen	5-5
Figure 5-4	Identification Scenario Selection Screen	5-5
Figure 5-5	Results Summary Screen	5-8
Figure B-1	Prisoner Intake Process	B-2
Figure B-2	Illustration of an Inmate Residence Pod	B-3
Figure B-3	Pod Activities.....	B-5
Figure B-4	Visitation.....	B-8
Figure D-1	Crime Scene Perimeter	D-2

List of Tables

Table 4-2. Personnel Assignments for Biometric Operational Technology Evaluation..	4-8
Table A-1. Summary of Biometrics in Correctional Facilities	A-3

1 Introduction

Mitretek Systems is a nonprofit company, chartered in the public interest that provides research and engineering support to all levels of government. The Center for Criminal Justice Technology (CCJT) is a “center of excellence” that provides unbiased technology expertise to the criminal justice community. Mitretek Systems operates the CCJT and receives federal funding to partner with state and local agencies in developing adaptable approaches for modernizing systems and practices that improve the efficiency, safety, and coordination of criminal justice agencies. In coordination with the Office of Justice Programs, National Institute of Justice, Department of Justice, CCJT annually selects projects because of their national significance and because they are critical to state and local criminal justice agencies of all sizes.

This report summarizes the project entitled *Biometric Authentication Credential in the Criminal Justice System—Applications to Access Control* conducted by CCJT under the National Institute of Justice (NIJ) and Cooperative Agreement 2001-LT-BX-K002.

1.1 Background

Criminal justice operations, particularly in support of Homeland Security, rely greatly on the correct identification of individuals who pose threats to national and local security. These operations also rely on providing access only to those individuals (e.g., corrections, court, and police officials; other first responders) who have been positively identified and authorized access to criminal justice system and related components. Positive identification of an individual can be no more effective than the up-front credentialing process – the individual is correctly identified and uniquely enrolled as one who has been approved for or is entitled to access.

Biometrics are defined as physical or behavioral characteristics that can be measured and compared by automated means to determine or verify the identity of an individual. A system that incorporates biometric identification may be used to facilitate the accurate credentialing of criminal justice officials and other individuals. A biometric uniquely binds the individual’s established identity to his or her physical person (i.e., bodily identity). Once an officer, for example, is credentialed, then positive identification of the officer may be performed rapidly and accurately or may be revised should the officer’s access profile need to be modified or revoked.

The *Biometric Authentication Credential in the Criminal Justice System* project began by examining the needs for, benefits of, and issues concerning integrating biometrics with the credentials of individuals associated with the criminal justice system (e.g., law enforcement officers, corrections officers, court staff, offenders, and visitors). The focus was on state, regional, and local criminal justice agencies since agencies at these levels are generally the first to initiate and provide criminal justice processing and services. Given the growing emphasis on Homeland Security, the need for secure and

interoperable credentialing between criminal justice entities and first responder and public safety agencies has become apparent. Programs to implement secure, interoperable identification credentials are already underway at the Department of Defense (DoD)—Common Access Card (CAC) [17-19] and the Transportation Security Administration (TSA)—Transportation Worker Identification Credential (TWIC) [20-25].

The Homeland Security Presidential Directive 12 (HSPD-12) issued by President Bush on August 27, 2004 mandates that the National Institute of Standards and Technology (NIST) creates a “Common Identification Standard for Federal Employees and Contractors.” The standard must be developed and promulgated by February 25, 2005. Federal agencies will then have four months to develop an implementation plan, followed by an additional four months to implement the standard where applicable. At the outset, this standard will “not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).” [12-16]

The *Law Enforcement Officers Safety Act of 2004* (PL 108-277, 7/27/04) permits current and retired law enforcement officers to carry concealed firearms. The subject individuals must possess appropriate identification credentials. H.R. 4914, *Aviation Biometric Technology Utilization Act*, was introduced in the U.S. House of Representatives on July 22, 2004. It requires the establishment of “a law enforcement officer travel credential that incorporates biometrics and is uniform across all Federal, State, and local government law enforcement agencies.” This bill appears to have died in committee. However, its content will likely be contained in expected homeland security legislation.

Access control is the fundamental application of biometric based credentialing that was explored in this project. Potential needs for officer and staff credentialing include controlling access to restricted or secure facilities or locations, controlling access to secure systems and information (e.g., maintaining critical infrastructure such as telecommunication facilities or computer data centers, submitting reports, accessing databases), and controlling access to services, equipment, or privileges. Operations within the criminal justice system, such as positively identifying visitors to prisons, individuals as they move about a prison—or between a prison and courthouse, and individuals who are released from prison, can benefit from the implementation of biometric identification technology.

1.2 Objectives and Scope

Given the apparent needs and trends noted above, Mitretek Systems’ CCJT, working under a cooperative agreement with the NIJ, Office of Justice Programs set out to team with a criminal justice partner and achieve the following primary objectives:

- Determine criminal justice entities and operations where positive identification of officers and staff is critical and where credentialing could improve operations related

to identification, access control, and data management. Examine the resulting benefits to resource allocation and public safety.¹

- Develop a technology demonstration and proof of concept for selected criminal justice applications of credentialing using biometrics. Provide lessons learned and address the feasibility, reliability, and scalability of the concept.
- Provide guidance to criminal justice agencies for potential applications of the proof of concept into criminal justice processes and operations. (A detailed, formal implementation guide is beyond the scope of this project.)

CCJT teamed with Arlington County, VA because of their first hand experience and lessons learned in leading the response to the 9/11/01 attack on the Pentagon and their special need to coordinate regularly with the multitude of Federal, State, County, and City criminal justice agencies in the Washington, D.C. metropolitan area. Arlington County staff were also very progressive in their thinking and offered enthusiastic support to this project.

1.3 Approach

The first step in this project was to make initial determination of criminal justice entities and operations where positive identification of officers and staff is critical and where credentialing could improve both the conduct and security of operations. Extensive research was conducted on current credentialing operations at criminal justice agencies – their strengths and weaknesses. Table-top exercises of end-to-end criminal justice processes during specific scenarios were performed by CCJT team members. The exercises examined various criminal justice entities, operations, systems, and other interfaces that require positive officer or staff identification. Examples included: an officer conducting a traffic stop, following the case through to adjudication; end-to-end crime scene investigation; end-to-end operations associated with a possible terrorist attack; and day-to-day operations. Simultaneously, research into credentialing and biometric applications underway at other government agencies and commercial companies was conducted to gauge costs, implementation, and lessons learned. An additional, major component of the research determined current and emerging technology applicable to criminal justice operations. Limitations of the technology were also factors.

We then sought to partner with an agency that had needs that might be addressed by biometric authentication credentialing, had the ability and desire to help identify and evaluate their needs, and was willing to apply their professional expertise to the development and evaluation of the proof-of-concept. The Arlington County, VA Office of Emergency Management, Police Department (PD), and Office of the Sheriff were chosen. The Arlington County Detention Center and PD were visited to obtain a first hand look at their operations and to identify potential, specific applications of biometric

¹ Where positive identification is critical, a single biometric based identification credential can provide a consolidated approach to identification (i.e., credentialing), access control, and data management and eliminate the use of multiple forms of identification.

authentication credentialing. As a result of the preliminary research and partnering, the criminal justice domain focus for this project was narrowed to corrections and law enforcement and the application focus was narrowed to access control.

Basic concepts of operation were developed for law enforcement and corrections. Criminal justice operations with a potential need for access control using biometric authentication credentialing were further investigated and evaluated with regard to practicality, feasibility, and usefulness. The common elements of access control technology using biometric authentication credentialing shared by all of the potential operations were developed into a basic concept of operation for criminal justice operations. The basic concept is to grant access to a person who has been positively identified using a biometric as the means of identity authentication, and who has permission for that access, while denying access to a person who has not been positively identified or who does not have permission for access. Extensions of this basic concept were explored to assess the versatility of biometric technology to seamlessly accomplish multiple goals and enhance multiple operations, thereby simplifying multiple tasks across corrections and law enforcement.

Development of the basic concept into a proof of concept demonstration followed. The proof of concept demonstration was developed and tested at Mitretek prior to setup at Arlington County. The demonstration consisted of two parts—a limited three-week operational test of fingerprint matching technology and a table-top demonstration of several application scenarios. The operational test permitted Arlington County staff to experience the operational use of fingerprint matching technology and provide feedback to CCJT staff on the efficacy of and requirements for biometric technology in their operational environment. The table-top scenario demonstrations provided illustrations of how biometric technology could be used in specific applications of interest. These demonstrations provided a means to elicit Arlington County feedback concerning the feasibility of biometric based credentialing and requirements with respect to such factors as scalability, performance (e.g., throughput, reliability, accuracy), and interoperability. If desired, an extensive pilot to closely study the complete credentialing, authentication, and identification process in an operational environment could then be undertaken. Such a pilot would require significant lead time to obtain permission to access criminal justice data, various background information, and other resources and was beyond the scope of the current project.

The final step in the project was to develop guidance and a cost benefit tool to help criminal justice technology officers assess the feasibility of an access control program using biometric authentication credentialing. The tool was developed in Excel.

1.4 Organization of this Document

Section 1 provides an introduction to this report, including the objectives and scope of this project and the approach taken to meet these objectives. An overview of biometric and credentialing technology, a description of possible applications of this technology to

law enforcement and corrections, and a summary of key U.S. government credentialing programs currently being implemented are provided in Section 2. Concepts and applications to Arlington County of biometric authentication credentialing for access control are presented in Section 3. Section 4 details the proof of concept testing and technology demonstration conducted with Arlington County. An analysis tool developed to assess costs and benefits associated with implementing a biometric authentication credential is described in Section 5. Conclusions are presented in Section 6. Following the main report is a list of references used in this project, five appendices containing supplementary information concerning the applications of biometrics to correctional facilities and critical incident management, and a list of acronyms used in this report.

2 Biometric Credentialing Technology and Applicability to Access Control

This section begins with a basic overview of biometric technology. Background information on credentialing and biometric based credentialing programs, and a description of potential applications to law enforcement and corrections follow. References that provide more detail have been included at the end of this document.

2.1 Biometrics

Biometrics are defined as physical or behavioral characteristics that can be measured and compared by automated means to determine or verify the identity of an individual. To be useful as a biometric, the characteristic must exhibit the following three properties:

- **Uniqueness** – characteristic must serve as a unique discriminator among individuals
- **Permanence** – characteristic must persist over a sufficient period of time such that it is not affected by processes such as aging or disease
- **Collectability** – characteristic must be collectable or measurable in an automated, non-invasive fashion.

Figure 2-1 below illustrates the generalized operation of a biometric system.

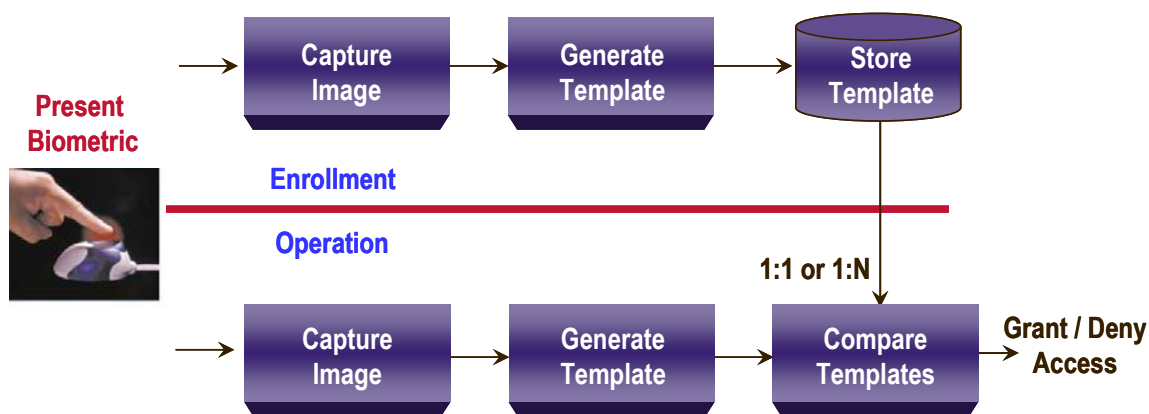


Figure 2-1. Operation of a General Biometric System

The three basic approaches to biometric matching are *authentication* (verification), *identification*, and *forensic analysis*.

- **Authentication** — generally involves the comparison of a newly presented biometric with a single reference biometric. The reference biometric may be stored, for example, in a central database or on an individual's identification card or other token. A subject presents to the biometric system claiming to be an individual previously enrolled in the system. A one-to-one comparison is made between the template created from the newly presented biometric and the stored reference template corresponding to the claimed identity.

- **Identification** — involves the comparison of a newly presented biometric with more than one (tens to tens of millions, or more) reference biometric, a process referred to as one-to-many matching. An identity is not assumed or claimed for the individual whose biometric is presented. A match will indicate the *identity* of the individual whose biometric was presented to the system.
- **Forensic analysis** — is typically an identification process in which biometric samples that are either incomplete or of sub-optimal quality are searched against a reference database to determine the identity of the individual. The use of biometrics for forensic analysis is generally associated with criminal investigations or surveillance operations conducted by law enforcement officials.

The most prevalent biometric technologies for non-forensic applications include fingerprint and palm print imaging, facial recognition, iris imaging, hand and finger geometry, and speaker identification. Less commonly used technologies include retinal imaging, gait analysis, dynamic signature analysis, hand vein patterns, body odor, ear geometry, and skin spectroscopy.

Of special note regarding biometrics is that the process of matching of a newly presented (“live”) biometric sample against a reference (enrolled) sample is probabilistic with an associated (usually very small) error probability. It is so unlikely that two biometric samples will be identical that an exact biometric match should be suspect and rejected for further investigation. This behavior can be contrasted with the matching of passwords, for example, where a match requires that the enrolled and presented passwords be identical. References [39-43] provide additional background on biometrics.

2.2 Credentialing

The American Heritage Dictionary defines the term *credential* as “that which entitles one to confidence, credit, or authority.” *Credentialing* as used in the context of this project is the process of compiling and storing information about an individual on a card, device, or other personal medium that remains with the individual. (The credential information may also be stored in a database for backup and/or subsequent verification purposes.) The information may be stored on the personal medium in human-readable and/or machine-readable format. The use of machine-readable formats can result in credentials that are more reliable, more secure, and more useful. This project focused on credentialing of individuals, although retailers, for example, use credentialing (e.g. shipping and storage information) for their products. A credential is a collection of information that describes an individual and typically contains an individual’s personal and employment-related information such as name, employer, address, job title, access privileges and authorizations, licenses and certifications. A biometric is one type of credential and can be used to bind an individual’s bodily identity to his/her informational identity. Other credentials may be contained in a standard report form used by an agency (e.g. birth certificate, social security data). Credentials may be stored electronically in formats that vary across organizations. Information contained in the credential may be used to grant or deny access to information (logical access), to a place (physical access), or to a service or privilege.

When designing a credential, the specific information elements to be collected, what information needs to be human and/or machine readable, whether to include a biometric and the type(s) of biometric to use, and the credential medium are application dependent. Design decisions can be quite complex as they are based upon a wide range of end-to-end operational system factors and requirements such as the following:

- Required credential information content
- Credential integrity and security
- Interoperability among multiple organizations
- Support infrastructure complexity and cost
- Credential medium and associated reader cost
- Credential medium durability
- Initial system size and anticipated growth (scalability)
- Time necessary to read, validate, and interpret the credential
- Operational environment (e.g., lighting, temperature, humidity, access to electrical power)
- Human factors

While a machine-readable credential has many benefits, the infrastructure required to support such a credential should not be underestimated. Included in such an infrastructure are effective means to update and revoke credentials. Updating and revocation of credentials becomes more complex the more agencies and systems are involved.

There are three fundamental functions associated with the credentialing process:

- **Enrollment**

Credential creation or enrollment is the first step in the credentialing process and its accuracy is critical. Enrollment includes collection of information pertaining to the individual, verification that the information is accurate and belongs to the individual, initializing the card/device on which the credentials will be stored, and recording the individual's information on the card/device. The next step in the enrollment process is ensuring the information can be retrieved from the storage card/device and that the information has been stored accurately. The enrollment process must be performed only by individuals authorized by the credential-issuing organization to do so. The individual to whom the card/device is issued must also be trained on proper care and use of the card/device.

- **Update and Revocation**

The update function is similar to the enrollment process and includes collection of additional information pertaining to the individual, verification that the information is accurate and belongs to the individual, recording the individual's updated information on the device, and ensuring the information can be retrieved from the storage card/device and that the information has been stored accurately. Authorized access is required to update an individual's credentials. The frequency with which the biometric is updated depends partly on the longevity of the biometric, commonly referred to as "template aging."

- **Reading and Interpretation**

An authorized credential reader (i.e. on a door) or an authorized individual (i.e. an authorized individual using an authorized computer) may read the machine-readable information stored on the credential to grant or deny access to a place, to information, or to a service/privilege. Machine readable credential information may be protected or encrypted so that it may be read only by pre-authorized computers/individuals. Queries may also be made to check information stored on the device or as part of routine maintenance.

There are other technical factors to consider for a biometric authentication credentialing program: the role of databases for storing biometrics and credentials; database structure, size, and composition; database stability; card or device used to store the credentials; process by which the individual will be authenticated and/or identified; and location of devices used to examine the individual's credentials.

- The role of databases for storing biometrics and credentials of interest here deals with privacy and protection of personal information. It may be generally accepted that in a criminal justice environment, employees (officers and civilians) and inmates would have significant information and biometrics stored in databases. However, privacy concerns most likely limit the storage of biometrics and credentials for visitors to the criminal justice systems.
- Database structure, size, and composition are determined by the application, and specifically by the number and characteristics of individuals who will need access. For example, access to an officer's patrol car may require that only the officer, the partner, and other limited set of personnel (i.e. maintenance staff, supervisors) have their information stored in a database of valid users for that patrol car. On the other hand, access to multiple buildings may require a larger database of individuals who have been granted access. Search time when operating in an identification mode (one-to-many search) increases with database size. Techniques such as database partitioning may be useful to reduce search time and increase reliability. Additionally, access rights will generally be assigned on an individual or role basis. For example, some individuals will be granted access to only certain parts of a building. These access rights will need to be reflected in an appropriate database.
- Database stability must be considered as part of the credentialing process. Depending on the application, the list of individuals may need to be updated frequently. While the list of officers with access to a given patrol car may be fairly static, managing an access list for control of multiple critical incident scenes and across multiple jurisdictions during an extensive investigation will be dynamic.
- The card/device that may be used to store an individual's credentials is also an element of the credentialing process and depends on the amount of information to be stored on the card, as well as the card security and durability required. The card may be contact (card must be inserted into the reader in order to be read) or contactless (card need only come within proximity of the reader to be read). One option for a contactless card/device, is one using radio frequency identification (RFID) technology, where credentials may be encoded in the card or device and read from very short distances (a few inches) to up to 90 feet away. [35-37]. Magnetic stripe

cards are contact cards and can hold 125 bytes of data. A card with a two dimensional (2D) bar code can store, typically, up to 1850 bytes of data. Smart cards can contain a memory chip that can store, typically, up to 64K bytes of data, may be contact or contactless. Smart cards may also contain a microprocessor. Optical memory cards store up to 2.8 Megabytes. Additional cards or storage devices may hold varying amounts of data. For reference and comparison, a single fingerprint image may require 90K bytes or more of storage, a compressed fingerprint image may be stored in 6K to 10K bytes, and a fingerprint minutiae template may be stored in 200 to 500 bytes. References [44-46] provide additional information on card technology.

- Another factor to be considered in the credentialing process is the method(s) and process by which the individual will be authenticated and/or identified. The process by which an individual's identity is verified and the individual's biometric based credentials are read may rely solely upon the individual's live biometric (i.e. the scan of the individual's fingerprint to unlock a door) or solely upon the individual scanning of his or her card/device encoded with his or her biometric. Alternatively, as is the strategy taken for this project, the individual may need to present both the biometric encoded card/device and the live biometric for comparison to one another. Matching of the encoded and live biometric implies authentication of identity.
- Location(s) of the devices to examine an individual's credentials to confirm identity and/or grant or deny access should also be taken into consideration. These devices may be stationary, such as with a door reader to gain access to a room or building or in a patrol car to access the mobile data computer/mobile data terminal (MDC/MDT). On the other hand, the perimeter of a critical incident scene may change, sometimes rapidly, over the course of an investigation. Portable devices would be beneficial in such a situation.

2.3 Potential Applications of Biometrics and Credentialing in Law Enforcement and Corrections

Criminal justice agencies should take advantage of advances in technology when this technology enhances their core mission: *to prevent crime and ensure public safety*, which results in agencies successfully addressing community issues. Figure 2-2 depicts the relationships between corrections and police departments that may be strengthened to achieve common missions. Biometrics and credentialing may assist with the seamless weaving and validation of information through the criminal justice process to help establish such an environment. Law enforcement, because of their broad contact with the public, can serve as a primary information collection vessel for all of law enforcement. This underscores the importance of data collection (incident/offense, arrest, field interview, intelligence reports, and evidence) and the ability for criminal justices officers to retrieve this data in an efficient manner. A general discussion of potential applications follows, with details of a specific concept provided in Section 3.

Biometrics may be used to facilitate the accurate credentialing of the five basic groups of individuals found in the Corrections and PD environments:

1. Sworn Personnel (Police Officers, Correction Officers, or Deputy Sheriffs)
2. Facility Staff (medical, administrative, food service, cleaning, etc.)
3. Inmates (suspects, detainees, or sentenced prisoners)
4. Official Visitors (attorneys, etc.)
5. General Visitors (friends or relatives of inmates, vendors, etc.)

Biometric authentication credentialing will be most useful to sworn personnel if used to control access to buildings and rooms, information, privileges/services, critical incident scenes, police department facilities, jail and court areas, as well as the escort of individuals. High accuracy biometric access devices could alleviate the need for centrally-controlled access systems requiring operator intervention to open doors. Additionally the biometric could be used to help determine officer location (in a building or on at a critical incident scene) by determining the last secure room that was accessed by the officer. Therefore, in the event of an emergency, officers can be located and provided needed support. Automated door opens and lock-ups could be provided based on validated identification, negating the need for the officer monitoring cameras to open

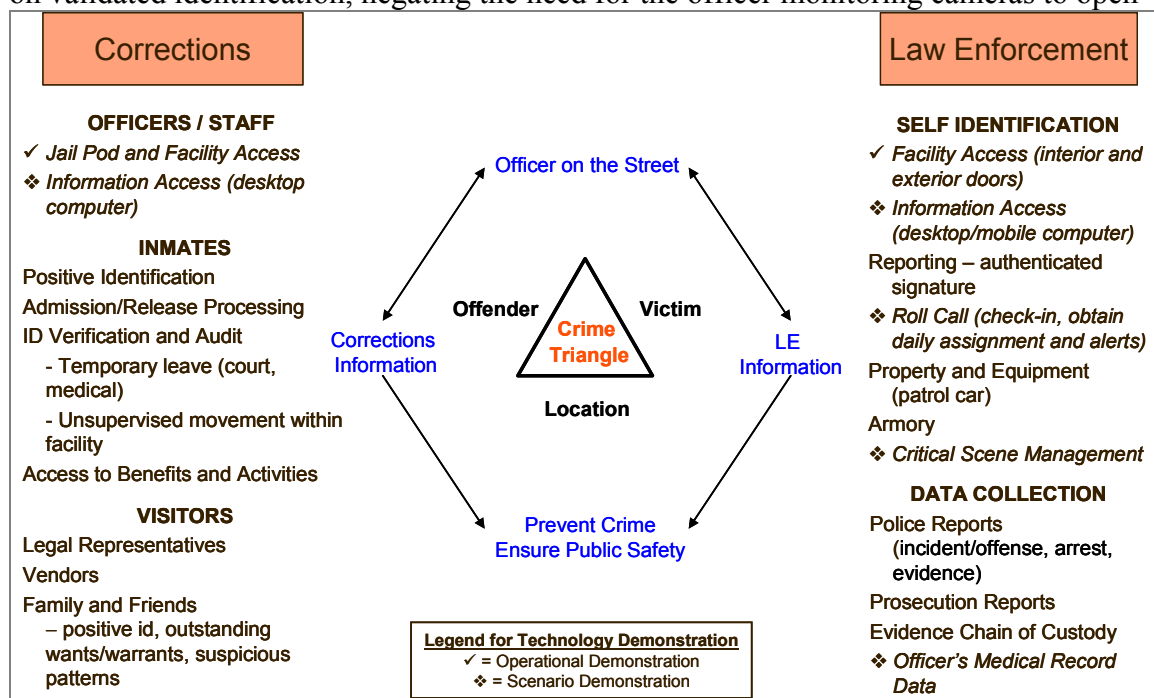


Figure 2-2. Applications of Personal Identification in Corrections and Law Enforcement

and close passages within the facilities. It frees up the monitoring officer to watch for safety violations or safety concerns rather than for door open and close requests. An additional application of the basic concept for officers is roll call. Officers may reliably and securely check in and check out, receive assignments, alerts, and crime data in association with their biometrically authenticated credential.

It should be noted that the biometric credential, which is part of an identity management infrastructure, is used in conjunction with an access control infrastructure. Such an infrastructure is typically software controlled and can limit an individual's access

authorization to specified dates and times.

Inmate biometrics and credentialing would be most beneficial in validation of inmate identity upon arrival and release, thereby reducing the possibility of improper releases. Additionally, inmate movement could be monitored within dormitory spaces and access restricted to specific locations (cells) at specific times. Access control and monitoring could be expanded to determining access permission and monitoring for inmate movement to legitimate areas such as wash rooms, laundry areas, healthcare and counseling areas, general visiting areas, legal or attorney visiting areas, recreation areas, dining areas, medical services, and courts, to name a few. Inmate biometrics and credentialing can also be used to track inmate attendance at required counseling sessions or other events, as well as for head counts at meals or roll calls. Biometric authentication can be particularly effective and useful for trusted inmates who are permitted to move about a facility within specified guidelines unescorted.

Official Visitor biometrics and credentialing can also be applied, similar to Facility Staff usage. Official Visitors can be allowed access to certain areas at certain times under access control. Location of visitors can be monitored without operator intervention. Official visitors usually require easy access to booking areas, interrogation rooms and legal visiting areas. General visitors typically have restricted access to designated visiting areas at designated times under some form of supervision.

General Visitor credentialing is useful for reducing workload for facility staff to control access to visiting areas. Jail visitations are a rich source of investigative information and often provide the most up to dates, names, locations, and gang movement. Additionally visitor credentialing allows interrogation of existing local and state databases to see if Wants or Warrants are outstanding on the individual visitor. The list of visitors offers a data source of inmate associations and family. Establishing a biometric based file of credentials on visitors provides investigators an additional tool in identification of suspects and can aid in locates. Also, accurate visitor monitoring & access control can be applied to reduce unauthorized movement or analyze frequent visits or suspicious visiting patterns to a single facility or between multiple facilities. The visitor's biometric is linked to an identifying database. In the event of an incident in a facility or in the event of a questionable individual or delivery, the positive identification capabilities of the biometric will aid law enforcement in their investigation.

2.4 Biometrics and Credentialing Programs

A summary of Corrections programs that have implemented biometrics has been included in Appendix A. References [26-29] provide supplementary information.

As noted in the introduction to this report and described in greater detail below, several broad-scope U.S. government programs to implement interoperable, biometric based identification credentials are in progress:

- HSPD-12
- DoD CAC
- TSA TWIC

2.4.1 HSPD-12

The most recent and far reaching effort on the part of the federal government is HSPD-12, which was issued by President Bush on August 27, 2004. This directive mandates the establishment and implementation of a common identification standard for federal employees and contractors. [12] At the outset, this standard will “not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).” Under its “Personal Identify Verification (PIV) of Federal Employees and Contractors” Project [13-15], NIST is working with stakeholders to develop the required identification standard, which will be called FIPS-201. The standard must be developed and promulgated by February 25, 2005. Federal agencies will then have four months to develop an implementation plan, followed by an additional four months to implement the standard where applicable.

The directive requires “secure and reliable forms of identification” that possess the following characteristics:

- “Is issued based on sound criteria for verifying an individual employee’s identity”
- “Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation”
- “Can be rapidly authenticated electronically”
- “Is issued only by providers whose reliability has been established by an official accreditation process”

On November 8, 2004, NIST released a draft standard for public comment. [16] The draft standard calls for a smart card containing electronically encoded biometric identifiers (two flat index fingerprints and a digitized facial photo). The card will also contain digital signature and encryption key data. The facial photo will also be visible on the front of the card. It is anticipated that this standard will influence identification programs at many state and local agencies as well, particularly those that interface regularly with federal agencies. State and local agencies may choose to adopt some or all of the standard. This may actually prove beneficial and improve interoperability when those agencies are first responders interfacing with other local, state, and federal agencies.

2.4.2 DoD CAC

The DoD has already begun implementing a high security credentialing standard for its employees and contractors. This standard is embodied in the CAC [17-19]. The CAC is consistent with the requirements of HSPD-12; some inconsistencies with the evolving NIST standard have been identified and are being addressed. More than five million cards have been issued thus far. The CAC is a smart card with photo image and use of public key infrastructure (PKI) to serve as identification and as a means for logical and physical access for a population of about 13 million employees and service women and men. Incorporation of a biometric is still under consideration. The CAC is revised every five years to minimize the opportunity for fraud.

2.4.3 TSA TWIC

The Transportation Security Administration (TSA) is developing the Transportation Worker Identification Credential (TWIC), a biometric based identification credential for an expected population size of about 12 million workers. [20-25] The TWIC will apply to all transportation workers who require unescorted access to secure areas at seaports, airports, rail, pipeline, trucking and mass transit facilities. TSA has completed the Technology Evaluation phase of TWIC and recently began the Prototype phase.

The TWIC will incorporate both a reference biometric (probably fingerprints) and one or more operational biometrics. The reference biometric is stored both centrally and on the credential and is used when issuing or renewing the credential to ensure that one individual is issued one and only one credential (identification mode of operation). The operational biometric(s) is selected by the local transportation authorities and is used to authenticate the individual's identity. Operational biometric templates are stored locally and/or on the credential. A variety of card types have been tested, such as contact and contactless smart cards, magnetic stripe, 2D bar code, and optical memory strip. The technology and evaluation phases of the program have been completed. Technologies to prevent tailgating/piggybacking and enhance surveillance are also being considered by TSA's distinct but related Airport Access Control Pilot Program (AACPP).

3 Biometric Credential Technology Applications

3.1 The Basic Concept

Smart cards, cards with 2D bar codes, and RFID tags, are currently common, portable forms of identification and may store a person's credentials. However, verification of the identity of the individual presenting the identification credential, such as via a personal identification number (PIN), or biometric verification via an external device is often not required. Therefore, the identification credential may be used by someone other than the person to whom the card was issued or read by an unauthorized person or system, allowing illegal access to a place, privilege, or information. An additional concern is the multiple badges most criminal justice officers carry to gain access to various buildings, rooms, information, and services.

There are two primary objectives around which the basic concept revolves:

- Biometric authentication of an officer's identity prior to granting the officer access or privileges
- The ability to store an officer's credentials on the identification card/device

Biometric authentication technology, using external hardware/software to scan a biometrically encoded card and compare a person's live biometric to a reference sample stored on the card, is readily available, as is the technology to compare a person's live biometric to a reference sample stored in a database. Also readily available are hardware and software to authenticate biometrically a computer user, in lieu of a password or PIN. The Basic Concept aims for an integrated approach to physical and logical (i.e., computer/information system) access. One card or device that addresses both objectives is the goal and is subsequently referred to as the *biometric authentication credential (BAC)*. The purpose of incorporating the biometric is two-fold: to accurately verify identity, and to render the identification card/device useless to anyone other than the officer to whom it was issued. To meet the objectives, the concept includes a BAC that works only if the legal owner biometrically "unlocks" or "activates" the BAC.

The purpose of storing credentials is to have a portable source of an officer's key information. There is one BAC on which the officer's biometric(s) and credentials are stored. The biometric(s) and credentials remain on the BAC with the officer and are updated, as needed, only by authorized security staff. This concept does not preclude the storage of the biometric(s) and/or credentials in official databases, if desired. However, database storage is not required. The fundamental benefit of the basic concept is the enhancement of the process for granting or denying access by allowing for accurate identification, self-identification, and improved data management. Additionally, the number of cards an officer must carry may be minimized if the BAC has storage space sufficient to store multiple credentials and multiple agencies/programs use the same basic BAC. The basic concept is depicted in Figure 3-1, Biometric Authentication Credential Concept.

Currently, criminal justice agencies like police departments and correctional facilities rely on either a hard paper folding credential (that includes a person's name, picture, and other identifiers such as height and weight) or a plastic card (that contains a picture and personal identifiers). These approaches store information in human and/or machine readable form and are used predominately to identify personnel. Typically, separate access control identification cards are used to control access to facilities (e.g., access through RF proximity door readers). The shortcoming of these credentialing and access control approaches, as noted earlier, is that the credentials or access cards are transferable to other individuals either intentionally through sharing, or surreptitiously, if lost or stolen.

The BAC concept has the potential to meet some of the needs of both law enforcement and corrections agencies in allowing them to control both physical and logical access with a tool that becomes unusable if not in the hands of the individual authenticated on the BAC (i.e., the individual to whom the identification credential was officially issued). This increases security and facilitates more accurate record keeping for an agency. This is especially important in criminal justice environments where valid identification is critical and access to information and physical locations is either monitored or restricted. The challenge of placing emerging technologies and innovative applications (including biometrics) into the criminal justice workflow is ensuring that the innovation does not stymie the smooth and efficient flow of agency operations, nor does it introduce a safety risk.

Biometric Authentication Credentialing Concept

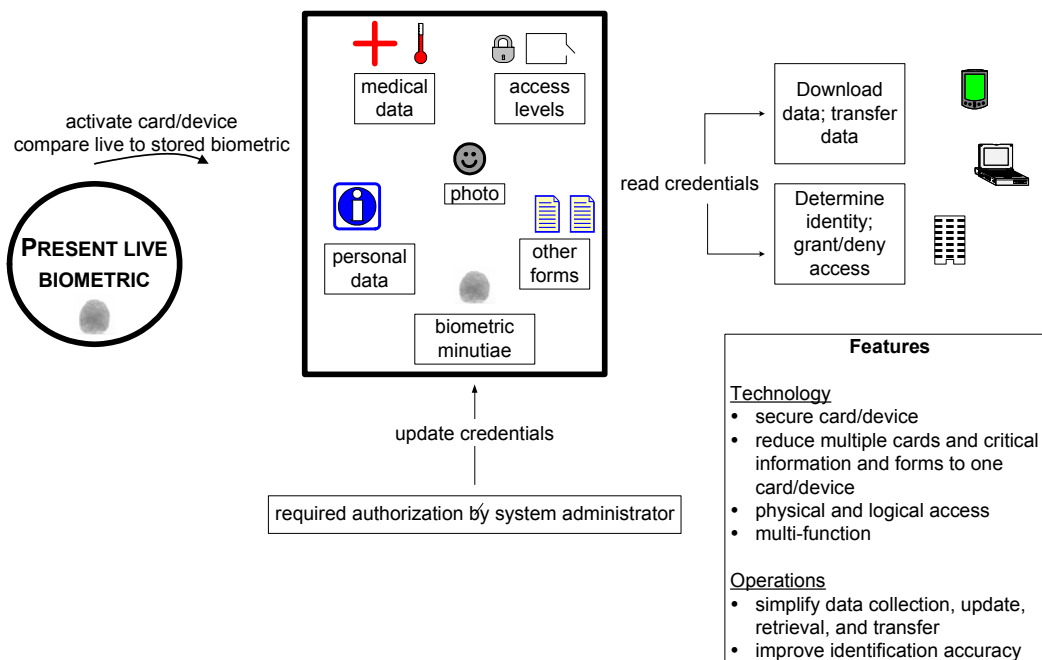


Figure 3-1. Biometric Authentication Credential (BAC) Concept

3.2 Application to Arlington County

The various applications presented in Section 2.3 were discussed with project partners and others working in the criminal justice community. It was the general consensus that applying the concept, as described in Section 3.1, to the inmate community was not feasible at this time. However, a description of how the concept may be applied to the inmate population is provided in Appendix C. Significant trust would need to be placed in the inmate to take care of the device. Applying the concept to facility staff and visitors presented some administrative and trust issues. Therefore, it was agreed that application of the basic concept would focus on sworn officers. Additionally, while initially of significant interest, explicit demonstration of the application of the basic concept to critical scene management, particularly large crime scenes, was beyond the scope of this project. However, a description of how the concept may be applied to the critical scene management is provided in Appendix D. The most fundamental problem associated with critical scene management is establishment of the perimeter, which was not the focus of this project.

The basic concept itself is limited in its usefulness if not properly paired with software applications that enhance its functionality. Therefore, throughout the remainder of this section, we assume that the biometric tool will be used in conjunction with various software applications that will increase substantially the applicability of this concept in the criminal justice sector. Potential extensions of the basic concept, with respect to law enforcement and corrections officers, are detailed below.

3.2.1 Extensions of the Basic Concept to Daily Operations

During a tour of duty, sheriff's deputies or police officers are required to show proof of identification on numerous occasions. The three primary types of applications requiring credentials (i.e., the term "credentials" used in the context of proof of identity) are:

- Physical access and identification for services or privileges
- Note: physical access and identification may operate in conjunction with one another since services may be offered within a secure site
 - Physical access – e.g., elevator access; garage access, access to multiple secured rooms within one or more buildings where each requires controlled access
 - Identification for services or privileges – e.g., time card systems used to log officers in and out of duty assignments; logging of and access to prescription medications for administration to inmates
- Roll Call –ensuring attendance and assignments
- Logical access –computers shared by multiple individuals that require the use of login usernames and passwords

Physical Access and Identification for Services

For both detention center staff and police department personnel, controlling access to secure locations and verifying identification is a significant security requirement. Both the Arlington County Sheriff's Office and the Arlington County Police Department have controlled access to their facilities. They ensure security by requiring personnel to present

their electronic access control cards when entering or exiting certain areas of the jail or police department. For example, the first opportunity for positive identification is usually the entrance into the secure facility to attend roll call. There are many factors that complicate the issue of access control. Some agencies may have multiple buildings requiring multiple badges, or elevators accessible to the public that lead to secure floors.

The BAC can improve access control and identity verification for officers and operations in a detention center and police department by:

- Providing the means to authenticate the presenter of an identification credential
- Requiring authentication to check in or check out property and/or equipment
- Monitoring the chain of custody of evidence
- Crime Scene/Critical Incident entry and exit personnel management
- Limiting access to sensitive facilities such as the armory or evidence room in a police department or the pharmacy in a corrections facility
- Automatically populating identification fields of required forms for accessing and tracking items such as equipment, property, and evidence
- Requiring personnel to authenticate before entering the facility or a segment of the facility such as a jail pod or holding cell to ensure positive identification
- Auditing staff movement in the facility by checking door reader logs

Consider the scenario where an officer needs to return equipment. The officer biometrically authenticates, presents the credentials, and access is granted to the armory. Additionally, the officer may verify identity to the armory attendant via the BAC. Upon returning the equipment, the armory attendant downloads the officer's credential related to the armory and updates the credential to show that the equipment has been returned. The armory attendant uploads the updated credential to the officer's BAC. The officer's credential may also be updated in the agency's database. The officer is able to retain his or her own credentials at all times. The time to complete the service may be shorter with the BAC than with other methods, such as paper or databases that may be difficult to manipulate. Most of all, the transaction has been credited to the correct officer, since the transaction is based on the biometric and combined with the credential.

Roll Call

Roll call is a mandatory attendance meeting for both sheriff's deputies and police department staff. It is during this time that deputies and officers "check in" for their shift and are assigned specific duties for that particular tour.

For some agencies, the current work flow begins when a deputy manually punches in at the time clock, and attends roll call. At roll call a sergeant will have prepared the shift assignment sheet with everyone's name and assignment. One of the functions of roll call is to confirm everyone's schedule, and ensure all assigned personnel are in attendance and provided an assignment for their shift. Once everyone is accounted for and assignments are confirmed, additional information (such as departmental administrative communications) is disseminated to the deputies. The roll call sergeant is responsible for ensuring the paper document with all personnel and corresponding assignments is

forwarded to payroll (usually on a weekly basis). The payroll staff is then responsible for manually keying the data for each employee.

The BAC has the potential to streamline the work flow process by:

- Recording accurately and electronically the personnel in attendance at roll call, including their time of arrival and check off, if desired. Some agencies use the honor code for officer attendance and may only be interested in which officers are present for duty.
- Supplying a record of officers in attendance to the computer aided dispatch (CAD) system
- Assisting administrative staff in documenting absenteeism, sick leave abuse, and tardiness
- Monitoring staff movement throughout their shifts (i.e., documenting when they “check in” and “check out” of various locations)

The BAC has the potential to benefit the officer specifically by:

- The roll call sergeant may upload the officer’s assignments to the officer’s BAC
- The officer on patrol may download the assignments, once in the patrol car, to the MDC
- The officer may electronically include assignment information with reports that must be written for the day

This process would eliminate much of the manual data entry and redundancy of typing names and assignments on paperwork.

Logical Access

Many of the computers used in corrections and police are shared by multiple individuals. Currently, departments require usernames and passwords to limit personnel access to files and other electronic information. Both the Arlington County Sheriff’s Office and the Arlington County Police Department use these methods for purposes of security.

The biometric device can improve the security of electronic data by:

- Restricting access to information (such as that found on a network or desktop computer), by using the biometric device to bypass or supplement the username and password interface
- Leaving a form of electronic signature (on a police report, prosecution report, or field report) when the biometric device is used

3.2.2 Other Considerations

As stated previously, the use of a BAC in conjunction with inmates or visitors was not considered in detail for this project. Likewise, the potential use of a corrections-related credential database in conjunction with apprehended suspects was not explored. [28] However, criminal justice agencies may consider extending the use of biometrics to Corrections in the areas of information/intelligence led policing and to the recidivism

patterns of ex-convicts. This could be achieved by increasing the information collected from suspects and those convicted of crimes, particularly biometric information, and making the reference information readily available to officers on patrol. An officer could take the live biometric of a suspect encountered while on patrol to confirm or “eliminate” the suspect’s involvement in a crime. The biometric of a suspect or convict could be used to positively identify that individual, even if that individual provides an incorrect name. The alias(s) could be linked to the biometric, along with other personal and arrest information stored in a database, which could in turn be used to automatically populate forms so that the officer would need to type only the elements of the offense.

4 Proof of Concept Technology Evaluation and Demonstration

A key goal of this project was to obtain criminal justice community input concerning the specific applications and requirements for biometric based credentials. To this end, CCJT conducted proofs of concept technology demonstrations with the Arlington County, Virginia Police Department and Office of the Sheriff. The Office of the Sheriff is responsible for security at both the Detention Center and the Courthouse. As illustrated by Figure 4-1, the Arlington County Police Department, Courthouse, and Detention Center are collocated.



Figure 4-1. The Arlington County, VA Police Department, Courthouse, and Detention Facility are Collocated

Consistent with this project's resource and schedule limitations, one operational test and several scenario demonstrations were conducted. An *operational* test of approximately three weeks was conducted to permit criminal justice staff hands-on experience with biometric technology in their day-to-day operations and permit them to provide feedback concerning the benefits, shortcomings, and technical/performance requirements concerning BACs. Based on suggestions from Arlington County staff, Mitretek then developed proof of concept software to demonstrate the following BAC application *scenarios* and elicit Arlington staff feedback:

- Create an employee credential that can be authenticated only with the employee's registered biometric

- Permit access to a secure physical site (where the access point may be guarded or unguarded), automatic logging of entry and exit times, and logging of property/evidence removal or return, or any special notes related to the individual's visit (if applicable)
- Authenticate and log an individual's presence for employee "roll call"

Vendor software did not become available within the time frame of this project, and so, although not demonstrated, Mitretek discussed with Arlington County participants the use of the BAC for accessing computer and network resources (commonly referred to as *logical access*). Figure 2-2 shows the scenario demonstrations conducted in this project amongst the wide variety of biometric credentialing applications to corrections and law enforcement.

4.1 Technology Selection

4.1.1 Background

As is evident from the various U.S. federal government programs in progress to develop interoperable identify credentials (e.g., Department of Defense Common Access Card, Department of Homeland Security Common Access Card, National Institute of Standards and Technology Personal Identity Verification Standard), many complex considerations and tradeoffs come into play when designing an identification credential and selecting its underlying technologies. General considerations include security, scalability, interoperability, technical functionality and performance, operational environment, durability, human factors, and cost. Cost must be assessed as the funds required to create, operate, and maintain the credentialing system in tradeoff against the potential cost associated with the risk of not having an adequate credentialing system in place.

A variety of materials (e.g., paper, plastic, foil, electronics), technologies (e.g., optical, electronic, software), and form factors (e.g., document, card, electronic device) have been used to create credentials. The most critical shortcomings associated with existing credentials relate to both credential issuance and post issuance use, as follows:

Credential Issuance

- Authentic credentials can be obtained using fraudulent identification documents
- Authentic credentials can be obtained through collusion (e.g., bribery) with issuer staff

Credential Use

- Authentic credentials can be shared or stolen; there is no positive means to assure that the individual who presents the credential is the individual to whom the credential was issued
- Authentic credentials can be altered with respect to the credential owner's identity, personal data, or authorizations and certifications
- Counterfeit copies can be made that appear to be authentic

This project's proof of concept activity was designed to address credential shortcomings that are encountered after issuance, and in particular the use of biometric technology to

assure that the individual presenting the credential is the individual to whom the credential was issued.

4.1.2 Fundamental Requirements

A criminal justice identification credential is used to identify an individual as an employee of a particular agency and indicate the individual's job position and authorizations/certifications (e.g., authorization to access property and information, or transport firearms; certification to use various hazardous materials and weapons). To determine the requirements of a given credential, various fundamental questions need to be addressed including the following:

- What general purposes is the credential intended to serve
- Which individuals and organizations will need to read and authenticate the credential
- What and how much information must be contained in the credential
- Is the credential intended to be read and authenticated through manual or automated means, and how rapidly must this process take place
- Under what operational circumstances will the credential be used
- In what environmental conditions will the credential be used and stored (e.g., temperature, humidity, lighting, noise, vibration)
- What are the risks and threats associated with credential use and misuse

Based on an assessment of the questions and considerations presented above with respect to the corrections and law enforcement environments, it was determined that the following capabilities needed to be provided by the technologies selected. Applicable (but not mandatory) technology solutions are indicated in parentheses.

- The ability to authenticate through automated means—
 - The issuer of the credential (digital signature)
 - The individual presenting the credential is the individual to whom the credential was issued (biometrics)
- The ability to store and update securely multiple sets of credentials (PKI)
- The ability to insure that the credential contents have not been altered (PKI)

Additionally, the credential needs to be able to perform the following functions:

- Authenticate an individual's access to both physical and logical entities, and also authenticate the electronic submission of reports
- Function rapidly and accurately
- Perform reliably in indoor and outdoor environments, and be sufficiently rugged
- Support issuance in the field for temporary use
- Support both standalone and networked operations
- Support a means for revocation, reinstatement, or modification as appropriate

It cannot be overemphasized that the credential, itself, is but one component of an

integrated identity and access control management system that is based on the complex, hierarchical integration of multi-jurisdictional policies and procedures with an assortment of technologies.

4.1.3 Description of the Selected Technology

To explore the issues and requirements described above and to provide Arlington County staff with hands on experience with biometric technology, CCJT selected the Privaris Biometric Personal Identification Device (BPID™) low frequency Bluetooth² (LFBT) model as the basis for the proof of concept evaluation and demonstration. The Privaris BPID™ security device is shown in Figure 4-2. It measures 3” long, 1.4” wide, and 1” deep at its thickest point and weighs 1.5 ounces. Additional information on the device may be found in Appendix E and in References [30-33]. (In the remainder of this document, we will refer to the BPID™ LFBT security device simply as the BPID™ device.) **It should be noted that CCJT selected this device as an *example* of applicable technology. This selection does not and should not indicate CCJT’s endorsement of this product.**

Other technology approaches, including alternative biometrics and smart cards, could have been selected as well. However, the approach chosen was fully compatible with and transparent to Arlington County’s existing access control system infrastructure and permitted staff use of biometric technology without disrupting current operations and security policies. No changes to any of Arlington’s hardware or software were required, other than registering the appropriate “card codes.” Had smart cards and fingerprint biometrics been used, for example, it would have been necessary to install smart card badge readers with integrated biometric sensors at all relevant access points.



Figure 4-2. Privaris BPID™ Device

The Privaris device owner’s fingerprint(s) and other credentials are stored on the device and the device owner activates the device using a fingerprint sensor located on the device. There is no need to store the owner’s fingerprint image or minutiae in a database,

² Bluetooth is a specification for short range wireless data communication in the unlicensed 2.4 GHz radio frequency spectrum [ref. www.bluetooth.com]

unless required for other operations. Once the device is biometrically activated by the owner, an authorized RFID reader may read the facility and card code information on the device and grant or deny access to the owner.

Integrated components and features of the device include the following:

- Fingerprint capture sensor (Authentec AFS 8500, 250 pixels per inch resolution, electric field type of sensor) – live fingerprint is captured and compared with reference template(s) stored on the device; fingerprint data never leaves the device. See Reference [34] for more information on Authentec, Inc. capabilities.
- ARM-7 microprocessor and 1.5 MB of associated memory – run software including encryption and fingerprint matcher software
- 0.5 MB of memory available for user applications (e.g., credential or other data storage)
- Indala gendered RFID sensor (functions as a 125 kHz proximity card); other RFID genders (e.g., HID) are available
- Bluetooth v1.1 transmitter/receiver (for data communication)
- Data encryption engine (PKCS #1 v2.1, FIPS 46-3 Data Encryption Standard (DES/3DES), FIPS 197 Advanced Encryption Standard (AES), SHA-1, SHA-256, MD5, FIPS 140-2 level 2)
- User replaceable battery (3V lithium, CR2)

Figure 4-3 illustrates the conceptual layout of the Privaris BPID™ LFBT device.

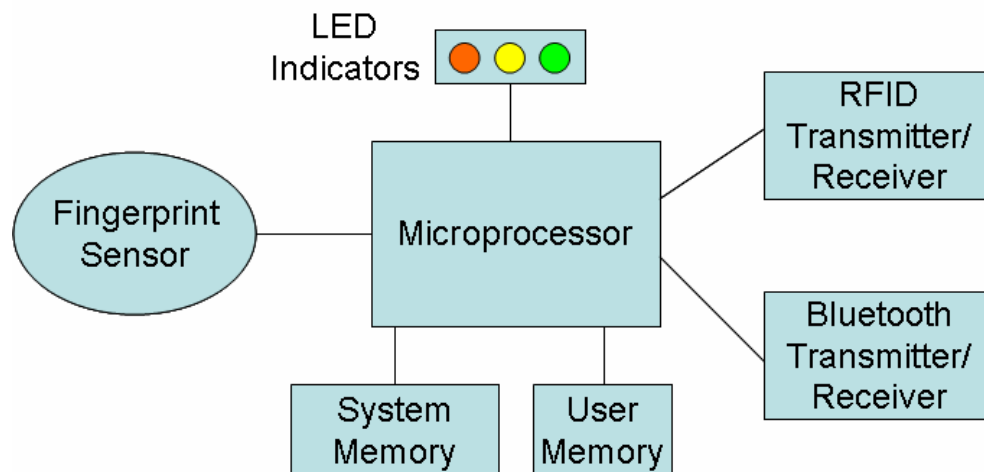


Figure 4-3. Privaris BPID™ LFBT Conceptual Diagram

Privaris has indicated that the BPID™ device is an evolving product. Upgrades to the fingerprint sensor, internal device design, construction, and microprocessor, which are planned for 2005, should enhance device performance considerably. A four-to-one reduction in fingerprint authentication time is expected. Privaris also plans to implement their technology in a variety of packages and form factors.

Operational Concept

The BPID™ device can be operated in two modes – low frequency RFID and Bluetooth. The device is placed in the RFID mode by pressing the power button once. The device is placed into Bluetooth mode by pressing the power button twice within two seconds.

When operated in RFID mode, once authenticated by a successful match of a newly presented live fingerprint with the device owner's enrolled fingerprint, the device appears to a 125 kHz RFID badge reader as if it is a 125 kHz RFID proximity card. However, RFID functionality is disabled prior to owner authentication. Therefore, this device will not function unless authenticated by the enrolled individual, whereas a conventional RFID badge can be used by anyone. To function with Arlington County's existing Indala formatted proximity badge readers and access control system, Indala-formatted BPID™ devices were specified. The BPID™ LF mode can be programmed to activate in one of three modes following biometric authentication:

- Following biometric authentication LF mode is active only for as long as the authenticated finger maintains continuous contact with the sensor
- Following biometric authentication LF mode is active for a fixed number of seconds (e.g., 10 seconds)
- Following biometric authentication, LF mode is active for a selected number of seconds following finger removal from the sensor

The third activation option was selected for the operational test.

The BPID™ device is operated in Bluetooth mode to transmit and receive data between the security device and a Windows® PC. The effective data transmission rate is approximately 15 KB/sec. It is in this fashion that one or more files containing device owner information (e.g., physical identity data, photograph, medical record data) can be written to and stored on the BPID™ device or read from the BPID™ device. Data may be stored on the device in encrypted form if desired. The BPID™ device's built-in encryption engine can be programmed to encrypt data before storage on the device and require device owner authentication before the data will be de-encrypted and released from the device. Alternatively or as an adjunct to on-device encryption, the PC-based software application can apply its own layer of data encryption.

Enrolling and Storing Device Owner Data

In conjunction with either an RFID or a Bluetooth transmitter/receiver that is connected to a PC, Privaris provides Windows compatible enrollment workstation software that is run on a PC to control the enrollment of an individual's fingerprints (up to six fingers—right and left thumb, index, and middle fingers) on the device. See References [32-33] for more information on the Privaris enrollment station user's guide. For each finger that is enrolled, the device captures five fingerprints, each of which must meet minimum image quality requirements. The images captured are processed to form a reference fingerprint template. A reference template is created for each enrolled finger and stored in the BPID™ device. Subsequently, during operational use of the security device, live

fingerprints are captured and compared with the reference templates. No fingerprint data ever leaves the device. It should be noted that a security key associated with the workstation (and any of an organization's related workstations) that enrolled the device is stored on each enrolled BPID™ device. This key is used to assure that all future device updates or erasures can be performed only on a workstation possessing the designated security key. An enrollment workstation that contains a security key that does not match the key stored on the device will not be able to access the device.

Development of Custom Application Software

Privaris also provides Application Programmer Interface (API) software that permits user-developed programs to control all device functions, including reading data (conventional Windows files) from device memory, writing data to device memory, and encrypting and decrypting data stored on the device. It is via this means that a systems programmer can develop custom software applications, for example, to create and store credential information on a BPID™ device or read this information from a BPID™ device and process it as desired. Stored data files can be tagged to require device owner authentication before reading of the file is permitted.

4.2 Operational Demonstration of Biometric Authentication Credentialing Technology (Fingerprints)

4.2.1 Purpose

The purpose of this operational demonstration was to permit Arlington County Sheriff's Office and Police Department staff to gain hands on experience with and assess the use of biometric technology during daily operations that currently require the use of a conventional RFID proximity card to control access. This test was not intended or designed to produce objective measures of biometric performance.

4.2.2 Approach

CCJT purchased four of the Privaris BPID™ LFBT devices configured in Indala³ format for compatibility with Arlington County's existing access control system. Arlington County security staff assigned temporarily four unused card identification numbers for use in the operational demonstration. Privaris encoded the four devices with Arlington's facility code and the assigned identification numbers. Therefore, once these card numbers would be activated in Arlington's access control system and associated with access control privileges, the four Privaris devices would function in the same fashion as Arlington's existing proximity badges. However, before each device could be recognized as an RFID badge, the device had to be biometrically authenticated by the assigned device owner.

As shown in Table 4-2, seven Arlington County staff participated in the operational demonstration during the time periods indicated. Individual usage of the BPID™ device ranged from 4 – 30 transactions per day, with a total of 376 BPID™ transactions during the

³ Indala is a manufacturer of RFID proximity cards [ref. www.indala.com]

three week evaluation period. Prior to participating in the evaluation, each individual was briefed on the goals of this activity, trained in the use of the BPID™ device, and enrolled on their assigned device. Arlington County security staff associated each individual's normal access control privileges with the newly assigned BPID™ number. If necessary, an evaluation participant could revert to using their proximity badge in the event of an emergency situation or failure of their BPID™ device. Following each individual's BPID™ usage period, the individual was asked to complete a short questionnaire and participate in an oral debriefing of their experience with and reaction to use of the BPID™ device and integrated biometric fingerprint technology.

Table 4-1. Personnel Assignments for Biometric Operational Technology Evaluation

Week 1	Week 2	Week 3
Sheriff's Office Security Administrator		
	Police Department Security Administrator	
	Program Manager	
	Corrections Supervisor	Corrections Deputy (Escort Officer)
	Police Commander (Information Technology)	Corrections Deputy (Escort Officer)

Week 1 was devoted to CCJT working with the Sheriff's Office and Police Department Security Administrators to ensure that each of the four devices being used in the evaluation functioned as desired. Also, the Sheriff's Office Security Administrator was given an opportunity to gain experience with the device in a "dry run" of the subsequent operational evaluation. The Security Administrators are responsible for identification badge issuance and operating and maintaining the facility's access control system.

Figure 4-4 illustrates use of the BPID™ device for doorway access control. Each of the individuals indicated in Table 4-2 used the device in this fashion to gain access to areas they would have normally accessed using their proximity badge. These areas, which included passageway doors, secure areas and rooms, elevators, and a garage, were all indoors except for the garage. The Corrections Deputies were responsible for escorting Detention Facility inmates to various locations around the Detention Facility and the Courthouse. For this test, the BPID™ devices were programmed to remain active for 10 seconds after authentication and finger removal, and so individuals were able to anticipate their need to authenticate the device prior to arrival at an access point.

4.2.3 Results

During the course of the operational demonstration, individual biometric device usage ranged from approximately four to thirty authentications per day. However, it should be noted that participants could have used their existing badge if and whenever they chose to do so. A summary of the comments and observations resulting from this limited operational test follows.



Figure 4-4. Police Officer Authenticates the Privaris BPID™ Security Device Using His Left Thumb to Obtain Doorway Access

Choice of Biometric

The test device employs fingerprint biometrics. When responding to an emergency, corrections officers many times need to wear latex gloves to prevent contamination with blood. The same situation could occur for police officers accessing a crime scene. Fingerprint sensors cannot detect fingerprints through latex gloves, and so an alternative biometric or other means of authentication would be required in such situations.

It was also noted that a hands free means for authentication would be better for officer safety. One of the participants suggested that speaker identification be explored for this purpose.

Biometric Enrollment

- There were no failures to enroll any of the participants' biometric data.

Biometric Authentication

- Fingerprint matching (authentication) occurred generally within 8-15 seconds. This time includes the time required to power on the device prior to each use.

- This response time, while adequate for applications that are not time critical is inadequate for time critical applications, such as responding to a fight in the Correctional Facility that would require no more than a two to four second total authentication response time.
- Test participants experienced the elevator reversing direction when they weren't able to authenticate in a timely fashion after entering the elevator. Authentication is required before floor selection is permitted.
- There was no quantitative data on the number of biometric false rejections (i.e., the live fingerprint of the true device owner did not produce a match with the reference (enrolled) data). However, participants reported experiencing some false rejections during testing—the devices would *time out* as designed and configured if no authentication occurred within approximately 30 seconds. The number of false rejections experienced was perceived more as an inconvenience than as a major issue with respect to events that were not time critical.
- Finger placement – minor changes in finger placement can significantly impact matcher performance; finger placement should be more natural/intuitive.

Effect of Training on Biometric Authentication Time

To get a sense for the impact of user training on biometric authentication time, authentication time measurements were made on two of the two Corrections Deputies both immediately following training and then five days after the start of device use. Five authentication time measurements (the time from powering on the BPID™ device until successful authentication occurred) were made for each of individual and then averaged. Based on this limited data set, the authentication time for the first individual improved from 14.2 seconds to 12.2 seconds for a 14% reduction in authentication time. For the second individual, authentication time improved from 12 seconds to 10.6 seconds for a 12% reduction in authentication time.

Device Form Factor and Construction

- Regarding law enforcement applications, concern was expressed that the device was somewhat large to carry in one's pocket or on a neck lanyard. Test participants preferred more of a card-like form factor.
- The device diverts the individual's attention away from their surroundings. The individual has to look at the device to see when device is ready for finger placement, where to position their finger, and when authentication has taken place. An audible tone occurring at the time of successful authentication might be useful. This situation jeopardizes officer safety.
- Participants indicated that the device should be waterproof enough to withstand wet weather and the dropping of the device in a sink, commode, snow, or water puddle
- Participants indicated that the device needs to be rugged and able to withstand being dropped or thrown to the floor, or rolled over or stepped on in a fight
- The sensor cover on the BPID™ device is too cumbersome and fragile to be effective during rapid response, high energy situations.

Feasible Applications for the Technology Demonstrated

Although the authentication response time of the technology demonstrated was not fast enough for time critical applications, the technology was deemed beneficial to access control applications such as the following:

- Guard tour – tours are random and take place during the night shift; it would be desirable to know exactly who has made the rounds and that all check points are visited; there are about 7 check points per housing unit and 12 housing units, resulting in at least 84 guard check points
- County maintenance staff – County maintenance staff circulate among all of the County facilities on maintenance and repair rounds. Paper logs are kept of the sites visited and work performed. It would be desirable to know who performed what actions and when, particularly with regard to mechanical rooms (e.g., wiring closets).
- Armory – distribution of weapons and ammunition
- Pharmacy – distribution of prescription medications and controlled substances to registered nurses for dispensing to inmates
- Central Control Room/Command Center – officers located in the Central Control Room control access to various locations via direct visual observation and via remote cameras
- Corrections Property Room – log staff in and out of this area where inmate property is maintained for safe keeping until they are released
- Evidence Room – log staff (and associated property) in and out of the this area where crime scene evidence is stored and tracked as part of the evidence “chain of custody”
- Equipment Distribution and Inventory Management – link credential with authorization to receive and use special equipment; integrate with a real time inventory management system
- Internal Affairs Office – provide controlled access to this office, which houses sensitive information
- Computer/Data Center

4.3 Scenario Demonstrations

CCJT and members of the Arlington County Office of the Sheriff and Police Department worked to identify a number of important applications and associated requirements for a biometric based criminal justice identification credential. However, the limited time and resources available to this project prohibited the development and implementation of application-specific operational pilots. Therefore, CCJT developed software that would illustrate some of these applications in proof of concept scenario demonstrations. These demonstrations could then be presented to criminal justice personal to elicit their feedback concerning the application of a biometric based credential to these applications.

CCJT created the following three scenario applications and reviewed them with

Arlington County staff:

- Creation of an employee credential that can be authenticated only with the employee's registered biometric
- Use of biometric based credential to facilitate access to a secure physical site (where the access point may be guarded or unguarded)
- Use of biometric based credential to facilitate employee "roll call"

As noted earlier, the use of the credential to secure access to information technology resources was of great interest. However, vendor software did not become available within the time frame of this project, and so, although not demonstrated, CCJT discussed with Arlington County participants the various aspects of this application, commonly referred to as *logical access*.

4.3.1 Creation of a Biometric Based Credential

Purpose

The purpose of this demonstration was to illustrate the process of capturing and enrolling an individual's reference biometric information and creating an associated credential containing data salient to the individual's identity, employer, certifications, and authorizations.

Approach

Depending upon the specific technologies employed and the intended applications, various approaches exist to creating and using a biometric based credential. For example, when using a smart card based solution, such variations include the following:

- The enrolled/reference biometric data may be stored on the card, at a local access point, or in a central database
- Given current technology, capture of the live biometric would take place off card; matching the live biometric to the reference biometric could take place on card, at a local access point, or on a central server
- The data components in the credential may include the following:
 - Personal identification information (e.g., photograph, height, weight, hair color, eye color)
 - Employment related information (e.g., employer, job title, employee identification number)
 - Certifications and authorizations (e.g., certification as a forensic examiner, authorization to transport firearms)
 - Digital encryption keys
 - Medical history (e.g., blood type, allergies, immunization record)
- Security treatment of the credential data – all or a portion of the data may or may not be encrypted and/or digitally signed by the credentialing organization; release of the data from the card may or may not require card holder authentication (biometric)

Biometric Enrollment

The design of the Privaris BPID™ device is such that fingerprint biometric enrollment (and subsequent matching) takes place entirely on the BPID™ device. This approach should allay privacy advocates' concerns that an individual's fingerprint data could be stolen and reused to falsify that individual's identity. As illustrated in Figure 4-5, the enrollment process is controlled by the Enrollment Station software, which is a commercial product of Privaris. The software lets the credential issuer configure various settings on the device that govern biometric verification and device activation (see Section 4.1.3). An individual may enroll up to six fingers in the device. It is good practice to enroll at least one finger from each hand. For the purposes of this demonstration, device activation (RFID) was programmed to last 10 seconds following authentication and when the user's finger is removed from the capture sensor. The individual assigned the device was asked to enroll both thumbs. More details of this process are described in Section 4.1.3. The Privaris enrollment workstation software maintains a database showing the initialization and update history of each BPID™ device enrolled by an organization.

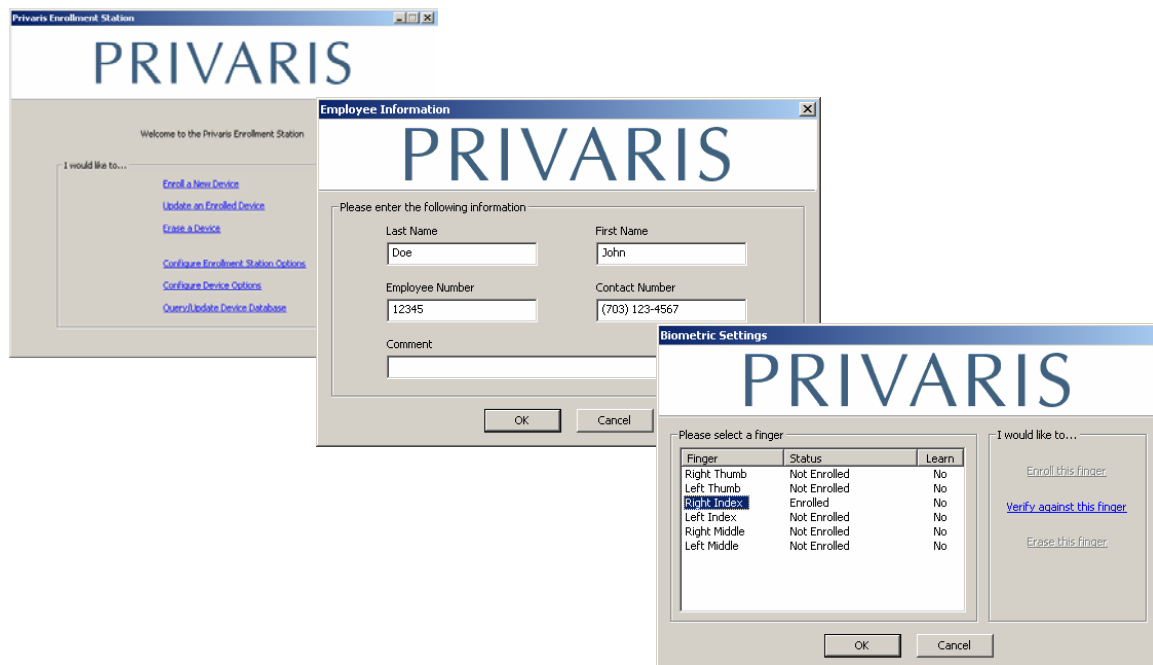
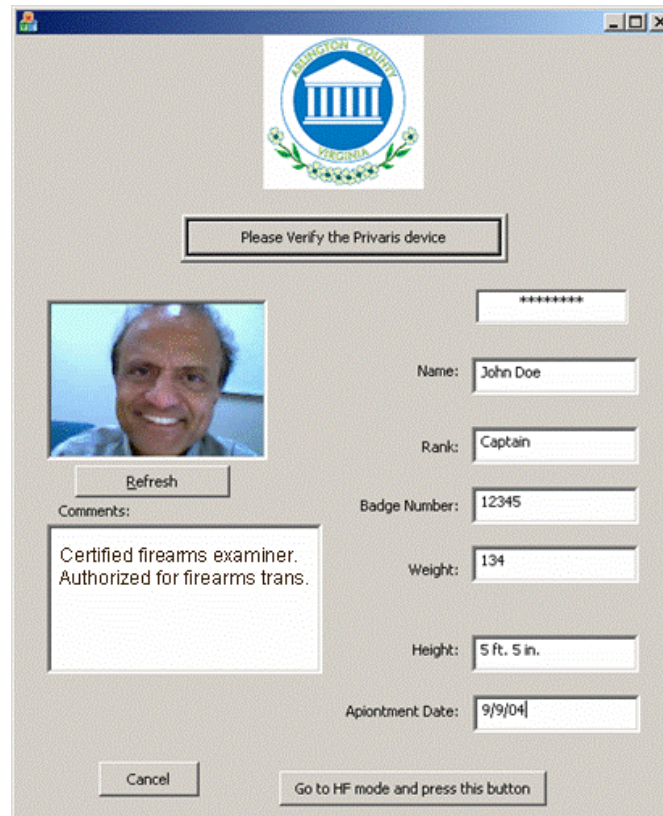


Figure 4-5. Illustration of Screen Sequence for Enrolling a Fingerprint Biometric

Credential Creation

CCJT created concept demonstration software intended for use by an enrollment station operator to create a sample employee credential. The software uses a USB PC camera (Logitech QuickCam v7.3) to capture a digital photograph of the employee. As illustrated in Figure 4-6, a form is then displayed for entry of the employee's name, rank, badge number, weight, height, and appointment date. A comments field is provided for the entry of optional information such as certifications and authorizations. The credential data is then transmitted to the BPID™ device via Bluetooth and stored in device memory as a conventional Windows data file. While not implemented for the purposes of this

demonstration to maintain software simplicity, this data file could have been digitally signed by the credential creator and/or encrypted prior to transmission.



Please Verify the Privaris device

Name: John Doe

Rank: Captain

Badge Number: 12345

Weight: 134

Height: 5 ft. 5 in.

Appointment Date: 9/9/04

Refresh

Comments:

Certified firearms examiner.
Authorized for firearms trans.

Cancel

Go to HF mode and press this button

Figure 4-6. Data Entry for Credential Creation

Results

The general approach to credential creation appeared to be acceptable. Of course, incorporation of technologies as digital signature to authenticate the creator and content of a credential will require a considerable infrastructure to support this capability.

With regard to the activation mode of the credential, the general feeling was that the credential, once authenticated by the presenter, should remain active only while the presenter's finger remains in contact with the sensor. This approach would minimize the possibility of one individual taking possession of and using another individual's authenticated credential.

4.3.2 Accessing a Secure Site

Purpose

This demonstration illustrates how a biometric based credential might be used to verify an individual's identity/credentials before granting that individual access to a critical incident site that has one or more controlled access points. Such sites would include the scene of a terrorist attack, a crime scene, or an incident involving the escape of hazardous materials. The basic approach demonstrated would apply equally well to validating a criminal justice official's identity before granting access to a secure facility, office, or repository such as a correctional facility pharmacy or a police evidence room. The demonstration was also designed to show how the credential can be validated with or without manual oversight, how an entry/exit log can be automatically generated, and how credentials can be issued in the field to individuals from outside a local jurisdiction who may need to access the given site on a sustained basis.

Approach

Using the Privaris-provided API, CCJT developed a software application that can be run on a mobile Windows computer outfitted with a USB camera, a Bluetooth transmitter/receiver, and an RFID proximity card reader (see Figure 4-7). This software application was designed with the assumption that a controlled access security check point has been established and that an entry/exit officer (EEO) monitors all passage through the check point and views on the computer display the credentials of each individual entering the access point. The individual wishing to gain access places the BPID™ device in RFID mode (presses power button once), authenticates, and brings the device in close proximity to the proximity card reader. The proximity “card number” is read from the BPID™ device thus identifying the individual to the system. The individual then places the BPID™ device in Bluetooth mode (power off device and then press power button twice) and the individual's credential file is uploaded wirelessly to the workstation screen for review by EEO, as illustrated in Figure 4-8. The EEO then indicates an accepted or refused entry and can enter any notes desired. If the individual wishing entry entered the site previously without a valid exit transaction, the program will provide an alert and request that an exit transaction first be completed.

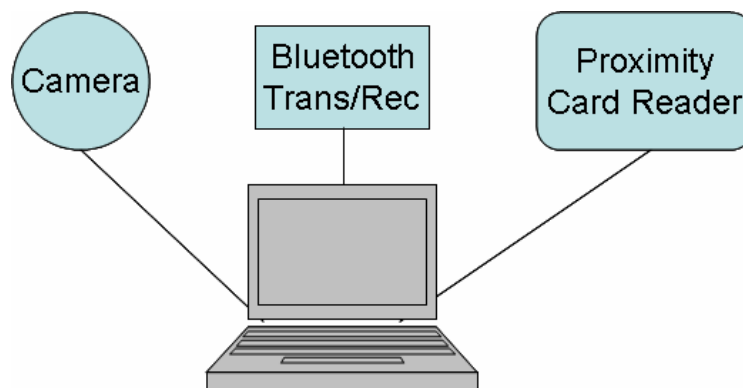


Figure 4-7. Configuration of the Mobile Access Control Station

Subsequently, when ready to exit, the individual places the BPID™ device in RFID mode, authenticates, and brings the device in close proximity to the proximity card reader. The proximity “card number” is read from the BPID™ device, thus identifying the individual to the system. The guard may add any notes desired, such as the removal of specific crime scene evidence. If the individual exiting did not have a valid entry transaction in the system, the program will provide alert the guard and request that an explanation be entered for the missed entry.

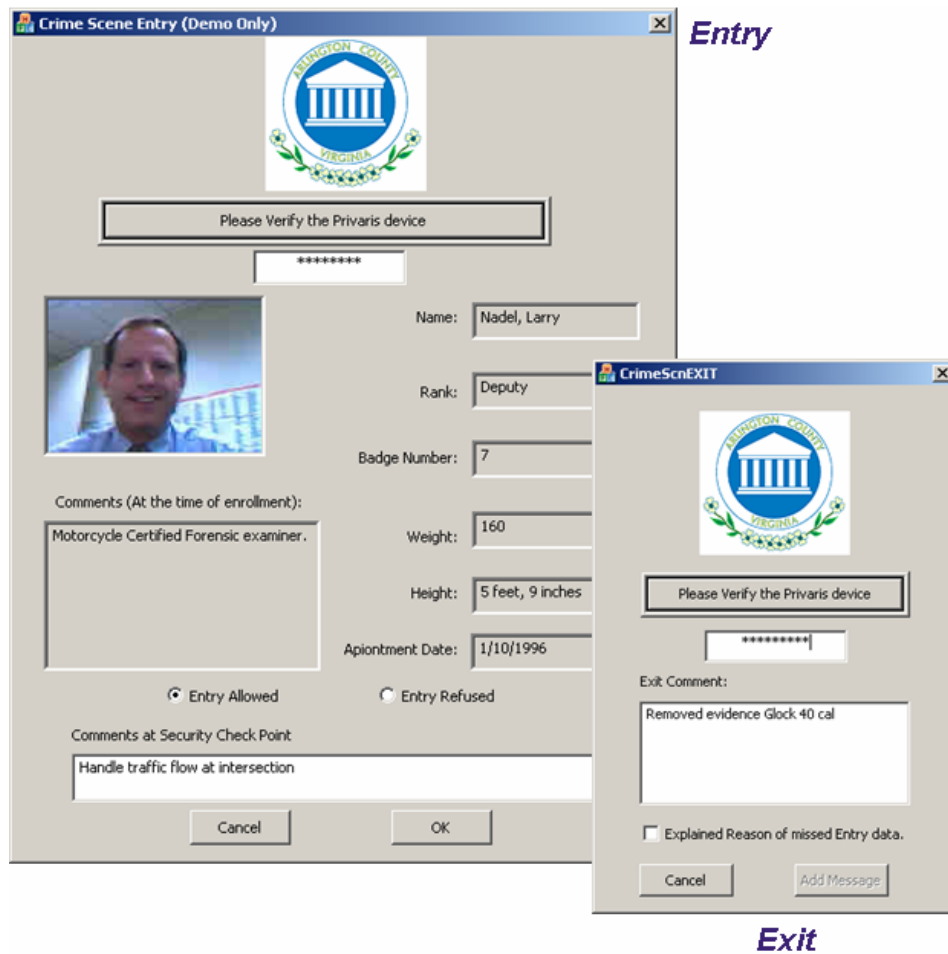


Figure 4-8. Illustration of Entry/Exit Workstation Screens

As illustrated in Figure 4-9, a database/log is automatically created of all entry and exit transactions to the given site. Simple, preformatted queries to the database can be issued to determine, for example, all those people who have entered but not yet exited the secure perimeter.

Critical Incident Anywhere, USA									
Name	Agency	Rank	Hair	Eyes	Ht. (in.)	Wt. (lbs.)	Date	Entry	Exit
Smith, Harry	Arlington PD	Ofc.	Blk	Brn	69	180	1/1/2004	1830	2158
Schader, Matt	Alexandria PD	Sgt.	Bld	Blu	72	200	1/1/2004	1835	
Woods, Greg	Alexandria FD	Prvt	Blk	Hzi	73	210	1/1/2004	1840	
Nadel, Larry	Fairfax PD	Dep.	Brn	Brn	69	160	1/1/2004	1841	
Williams, Brad	Alexandria FD	Prvt	Brn	Brn	72	210	1/1/2004	1843	
Johnson, Tim	Arlington EMS	Prvt	Blk	Blu	74	205	1/1/2004	1845	1900
Wilson, Tom	Arlington EMS	Lt.	Bld	Blu	69	155	1/1/2004	1845	1901
Doe, John	Fairfax PD	Capt.	Brn	Blu	65	134	1/1/2004	1850	

Figure 4-9. Illustration of Entry/Exit Log

Results

The approach demonstrated to authenticate entry and exit to a secure site received a generally favorable response. The following four points were raised:

- Biometric authentication time was too slow (i.e., > 2-4 seconds) when time was of the essence (note that authentication time was improved by a factor of 2-3 following a firmware upgrade made by Privaris after this testing and demonstration activity had concluded)
- This may not be the optimal temporary credential; loaned devices may not be returned; the devices (currently) can't be used elsewhere (lack of interoperability).
- Initial stage of a critical incident is chaos. This approach would be implemented after order has been established and would be used for sustained event. When dealing with a critical incident, first responders generally first tend to the injured and then secure the scene.
- The ideal solution/technology should integrate into current operations seamlessly.

4.3.3 Officer Roll Call

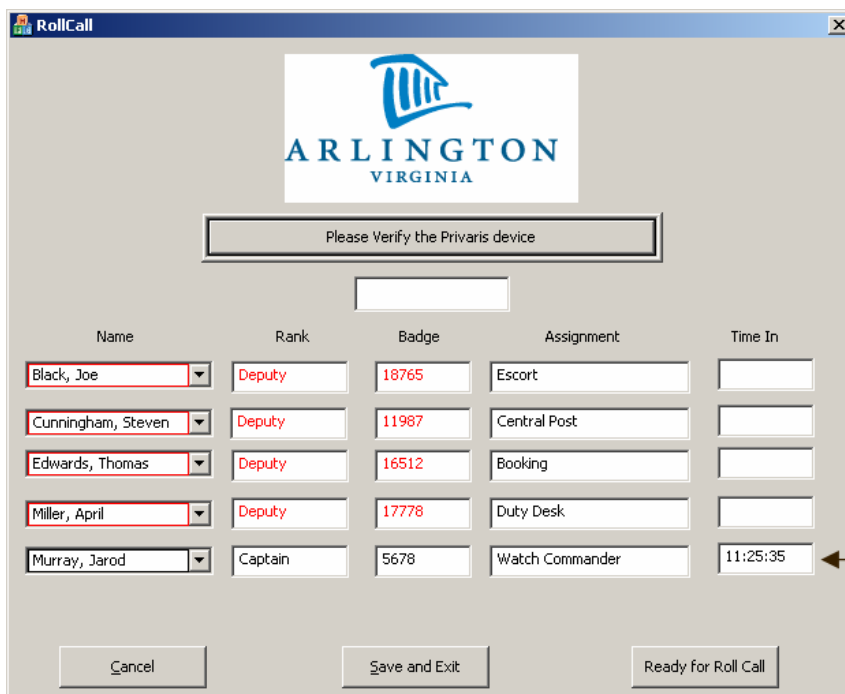
Purpose

This demonstration illustrates how a biometric based credential can be used to facilitate Officer Roll Call. In an operational system, an application such as this could be integrated with the time and attendance system to facilitate payroll processing.

Approach

Using the Privaris-provided API, CCJT developed a software application that can be run on a Windows computer outfitted with a USB RFID proximity card reader. To initiate a roll

call shift, the officer in charge is presented with a screen similar to that illustrated in Figure 4-10. Each drop down name box at the left side of the screen contains a list of all officers employed by the organization. The officer in charge makes a selection for each officer assigned to the shift of interest. Entries for rank and badge number are automatically populated in the table and colored in red. The individual's assignment is then entered. A variation of this approach could have been that each individual's previous assignment is automatically populated in the table, so that the officer in charge only has to enter *changes* to previous assignments. Once the roll call roster and assignments have been established, as each officer shows up for roll call, they would place their BPID™ device in RFID mode, authenticate, and place the device in close proximity to the RFID badge reader. The "card code" is read, the current time is noted in conjunction with the officer's entry, and the color of officer's rank and badge number text is changed from red to black. When roll call is ready to begin, the officer in charge can review the roll call list and readily determine those officers who are not present. Reassignments can then be made as necessary. The officer in charge may then print out and/or save the electronic log for future reference.



Name	Rank	Badge	Assignment	Time In
Black, Joe	Deputy	18765	Escort	
Cunningham, Steven	Deputy	11987	Central Post	
Edwards, Thomas	Deputy	16512	Booking	
Miller, April	Deputy	17778	Duty Desk	
Murray, Jarod	Captain	5678	Watch Commander	11:25:35

Figure 4-10. Illustration of Officer Roll Call Data Capture Screen.

Results

The approach demonstrated for Officer Roll Call received a generally favorable response. The following two points were raised:

- The approach demonstrated will greatly simplify the current process of manual record keeping
- The challenge will be integrating this application with the back end legacy time and attendance software

- This approach will support Computer-Aided Dispatch (CAD) operations

4.3.4 Computer/Network Access

Purpose

This application was intended to illustrate how the biometric based credential can be used to facilitate logging onto a standalone or networked computer and eliminate the possibility of shared, stolen, or forgotten passwords.

Approach

At the time of this evaluation, Privaris Corporation had work in progress with several computer security software vendors to develop software to permit logging into a Windows computer using the BPID™ device. Future software enhancements included use of the BPID™ device to facilitate digital signature and public key data encryption. Since the application software was not completed in time to demonstrate before the conclusion of this project, CCJT simply discussed the anticipated capabilities with Arlington County staff.

Results

The Virginia State Police is requiring more secure means for accessing information resources and so biometric authentication can go a long way to helping meet this requirement. The following two points were made:

- The anticipated capability was highly desired for use by both the Sheriff's Office and the Police Department.
- Computer hardware and software vendors (e.g., Microsoft® and IBM) are beginning to integrate biometric solutions into their product offerings.

4.4 Results Summary

The following points summarize the comments received and observations made during the technology and scenario demonstrations conducted with Arlington County staff:

1. Authentication response time, as demonstrated, was too slow for time critical applications; for such applications, response time needs to be no more than 2-4 seconds. The biometric based credential would be useful for a variety of applications that are not time critical, such as accessing the Pharmacy, Armory, or a computer.
2. Some false rejections were encountered by test participants; however, they were reported more as an inconvenience than as a problem
3. Hands free operation would be better, and mandatory in some cases. The need to look at the device to "fine tune" finger placement or determine if authentication was successful by viewing the LEDs diverts the officer's attention away from the matter at hand. This could result in a safety and security risk.

4. Fingerprint biometrics were chosen for use in this project. A fingerprint reader is not compatible with an individual wearing gloves. A multi-biometric or other alternative means of authentication is needed.
5. The role of human factors in product design and adequate user training is critical to the successful use of biometrics.
6. A key challenge is integrating the biometric solutions demonstrated with back end software and establishing an appropriate data infrastructure for department wide use and interoperability with other organizations/jurisdictions.
7. Additional infrastructure is needed to implement digital signatures and PKI, if desired.
8. Some of the project participants expressed concerns about the Privaris device size and form factor. Other individuals were satisfied with device size and form. Several officers noted that the device needed to be waterproof and durable with respect to physical shock.

5 Costs and Benefits for Basic Concept

As mentioned in Section 1, one of the goals of this project was to “Provide guidance to criminal justice agencies for potential applications of the proof of concept into criminal justice processes and operations.” Therefore, to enhance the lessons learned and guidance gleaned from the proof-of-concept development and results, a tool was developed with the goal of helping law enforcement and corrections assess costs and benefits associated with access control systems, with the “basic concept” described in Section 3.1 as a primary point of comparison.

5.1 Approach

The cost and benefit tool was developed as an interactive Microsoft® Excel model. The model was developed to perform the following functions:

- Present basic access control options
- Allow the user to estimate basic costs of access control systems specific to the user’s agency(s) or program
- Allow the user to determine potential (quantitative and qualitative) benefits and trade-offs with respect to different access control systems
 - Quantitative – time to complete operations and potential cost savings for specific operations
 - Qualitative – consequences of having, or not having, different access control systems may be wide-ranging with respect to cost of damages and may have extremely low probability of occurrence; these are better reflected qualitatively
- Present other factors to be taken into consideration when assessing access control programs

5.2 Model Assumptions

Various assumptions specific to model calculations and interpretation of results are posted on related worksheets in the model. The user is encouraged to read all assumptions carefully. Some of the key assumptions are listed below:

- The model generates costs over a five year period, the anticipated life of an access control system.
- Background checks for individuals issued access control badges must be thorough and diligent, as an agency would require them today. The process of background checks and identity verification, prior to issuance of access control badges is beyond the scope of this model and project. Verification of credentials and basic information is absolutely critical. Coupling this information with the biometric increases the level of confidence that the information and credentials actually match the individual to whom the credential was issued and as well as the individual who subsequently presents the credential.

- The basic concept and model focus on sworn officers. However, the model provides the user the option to include officers *and* civilian staff as the employee population to be included in the access control program.
- There are four basic types of regular employees affiliated with a program: sworn officers (staff); sworn officers (manager); civilian (staff); and civilian (managers). These include employees housed on site as well as employees housed off-site, employees from other agencies who regularly conduct business in the program, and contractors. Employees do not require escorts. In the model, all regular employees are issued access control badges.
- Physical access points may be uncontrolled or controlled. Uncontrolled access points may be open to the general public or open to all who have passed through a previous controlled access point. Controlled, physical access points may or may not have a security guard present. Guarded, controlled access points may be reserved for main entry points, such as a building or critical scene, and other highly secure areas. Unguarded, controlled access points may be reserved for other interior rooms where access is limited, such as a central control room or jail pod. Access to unguarded, controlled access points may be via electronic door readers or keys. Uncontrolled physical access points are not reflected in the model.

5.3 Model Description

The model consists of four main parts:

- Project Introduction and Model Information
- Model Input
- Results
- Additional Considerations

Each of the four parts contains multiple sheets and is described below. ***In the screen illustrations that follow, it should be noted that the data presented are illustrative and do not represent actual values for any specific organization.***

5.3.1 Project Introduction and Model Information

The *Project Introduction and Model Navigation* part does not require any input from the user. This part of the model consists of five sheets.

The first sheet is the *Welcome* page. The second sheet, *Map of the Model*, as shown in Figure 5-1, contains instructions to help the user navigate through the model and buttons linking the user to the various sheets of the model. The remaining three sheets contain extensive information about the model, as well as about identification technologies.

- The *Read Me* sheet contains basic information about how to use the model. A summary of all worksheets contained in the model is included.
- The *Purpose and Examples* sheet, which describes the types of benefits and hindrances to identification technologies. Potential costs and cost savings factors are listed.

- The *Scenario Options* sheet describes the features of four basic identification scenarios, including the device used for the proof-of-concept. These four system approaches are used throughout the model and are the basis for the model user to define an access control system. Further, potential applications of biometric based identification credentialing, and their benefits, are presented.

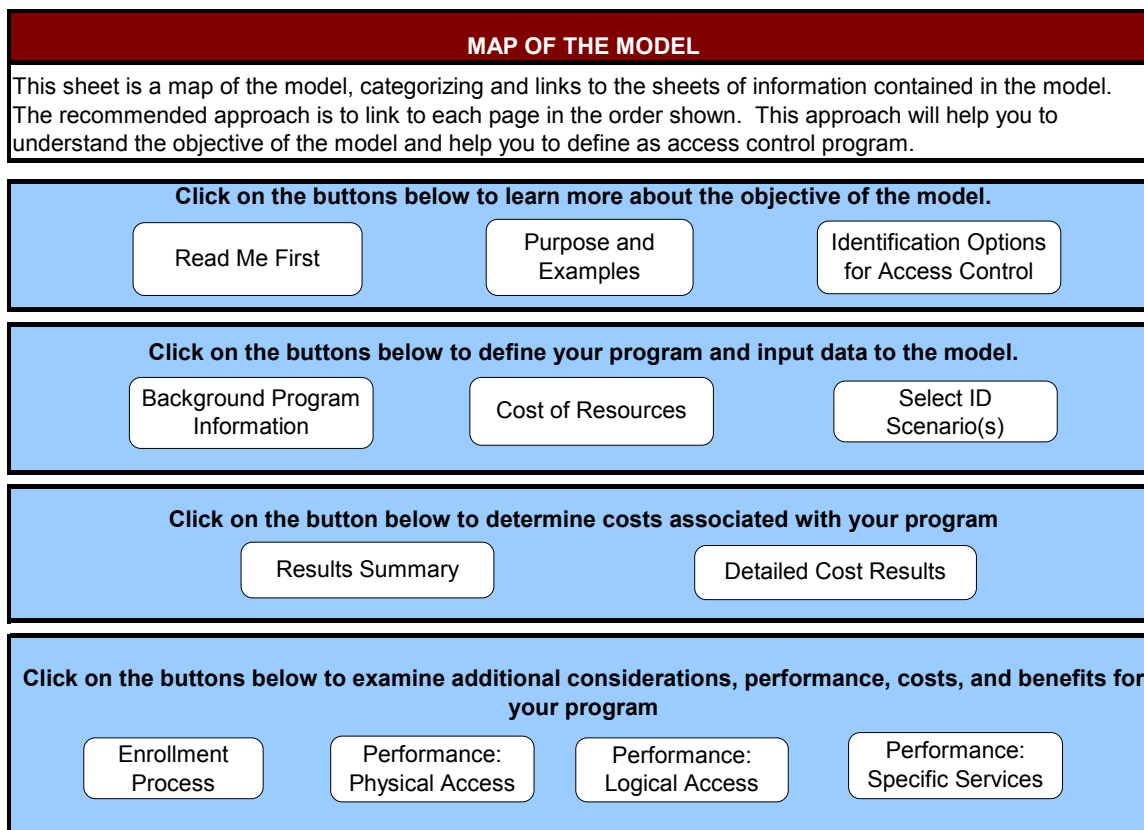


Figure 5-1. Map of the Model Screen

5.3.2 Model Input

The *Model Input* part of the model consists of three sheets and requires user input. Input should pertain to the projected access control program for which costs and benefits are to be measured.

- The *Background Program Information* sheet, as shown in Figure 5-2, asks the user for data related to the employee population make-up and size, number and types of access points, number of computers, and current identification program.
- The *Cost of Resources* sheet, as shown in Figure 5-3, is the input point for annual costs of various employee types, as well as the input point for rate of salary increase and employee turnover rate.
- The *Select ID Scenarios* sheet, as shown in Figure 5-4, is where the user defines the identification scenario options to meet agency/program operations by specifying the types of identifications needed. The model generates the number of different

identifications and door readers needed based on the users selections on the *Select ID Scenarios* sheet, and based on user entries on the *Background Program Information* sheet.

BACKGROUND INFORMATION ABOUT THE PROGRAM(S) OR AGENCY(S)	
<p>Instructions: On this sheet enter data about your agency or program for which you wish to estimate access control costs. With the exception of the request for current data below, you may enter current data or you may enter projected data. For example, you may enter data about your <i>future</i> employee population, future access points, and computer inventory. The model calculates costs reflecting your current program or your projected program, based upon the values you enter.</p>	
<p>Assumption: There are four basic types of regular employees affiliated with a program: officers (staff); officers (manager); civilian (staff); and civilian (managers). These include employees housed on site as well as employees housed off-site, employees from other agencies who regular conduct business in your program, and contractors. Employees do not require escorts. In this model, all regular employees are issued access control badges.</p>	
<p>Assumption: Visitors, such as the general public (inmate attorneys/counsel and inmate visitors); some contractors; and some employees of affiliated agencies (civilians and officers) are not reflected in this model. It is assumed that the current process for admitting and tracking visitors is unchanged and that visitors are not issued access control badges.</p>	
Describe Your Regular Employee Population	
Enter the number of officers/deputies who are staff in your program	200
Enter the number of officers/deputies who are managers in your program	100
Enter the number of civilian staff in your program	50
Enter the number of civilian managers in your program	20
Other: Enter the number of any additional individuals who need regular/permanent access to your facility	10
Total: This is the total number of employees needing both physical and logical access	380
Access Points	
Enter the total number of controlled access points needing security guards only?	3
Enter the total number of controlled access points needing door readers only?	20
Enter the total number of controlled access points needing security guards and door readers?	2
Total: This is the total number of controlled access points in your program.	25
Total: This is the total number of security guards posted at the controlled access points.	5
Total: This is the total number of door readers posted at the controlled access points.	22
Computer Inventory	
How many desk top and laptop computers are dedicated to only one user	50
How many desk top and laptop computers are shared by multiple users	100
Total: This is the total number of computers in your program.	150
Funding Sources	
Enter the total dollar available to help offset the cost of an access control program. Include grants that may be available (i.e. from Homeland Security, Department of Justice) or fees that your program may charge for services you provide.	\$1,000
Next Step	
<div>Return to Map of Model</div> <div>Go to Define the Cost of Human Resources</div>	

Figure 5-2. Background Program Information Data Entry Screen

Cost of Human Resources					
Human Resources by Type and Cost Projected Out Over Life of Access Control System					
Instructions: Enter the current, typical, annual, cost of one full time equivalent (FTE) for each type of employee. <i>Employee costs should be loaded to include salary and benefits.</i> Enter cost under Initial (Current) year only. Costs for Years 2 through 5 are calculated based on annual rate of salary increase entered below. When finished, follow the NEXT STEP instructions at the bottom of the sheet.					
Employee Type	Enter Initial Year Annual Salary and Benefits	Projected Employee Salary and Benefits By Year			
		2	3	4	5
Civilian employee - staff	\$75,000	\$78,000	\$81,120	\$84,365	\$87,739
Civilian employee - manager	\$105,000	\$109,200	\$113,568	\$118,111	\$122,835
Officer and Deputy - staff	\$75,000	\$78,000	\$81,120	\$84,365	\$87,739
Officer and Deputy - manager	\$105,000	\$109,200	\$113,568	\$118,111	\$122,835
Maintenance staff	\$45,000	\$46,800	\$48,672	\$50,619	\$52,644
Security Staff (responsible for ID management)	\$75,000	\$78,000	\$81,120	\$84,365	\$87,739
Miscellaneous Parameters		Enter Below			
Enter the annual rate of salary increase, in the box to the right.		4.0%			
Enter the number of hours an FTE actually works per year (allows for vacation, holiday, and sick leave). Total hours available are 2080, based on 40 hours per week times 52 weeks per year. The default is 1880 hours actually worked per FTE, per year: which takes into account holidays (10 days), vacation (10 days), and sick leave (3 days).		1896			
Enter the annual, overall, regular employee turnover rate in your program (%)		10.0%			
Enter the annual rate of inflation (%)		3.5%			
Next Step					
<div style="display: flex; justify-content: space-around;"> Return to Map of Model Go to Select ID Scenario(s) </div>					

Figure 5-3. Cost of Resources Data Entry Screen

Select Access Control Systems With Respect to Identification Scenarios and Door Readers		
Instructions: On this sheet you will define the type(s) of identification you would like for the employees in your program/agency. The primary identification scenario you define here will be applied to all employees, unless you specify an additional ID scenario at the bottom of this sheet.		
Selection of Primary Identification Scenario		
Would you like your employees to have a tangible card/device for identification? Note: if you answer "NO", the Scenario 4 - biometric only option is assumed, regardless of other entries below.	no ▼	
Would you like to use a biometric (fingerprint) to enhance verification of employees?	no ▼	
What type of sensor would you like to use to capture an employee's live biometric?	personal sensor ▼	
Where would you like to store an employee's reference biometric?	on card/device ▼	
Where would you like biometric matching to occur? This is where the biometric comparison software resides. The matching compares the live biometric to the reference biometric at time of identity verification.	on card/device ▼	
All 380 employees will use the primary ID scenario below, unless an additional scenario is defined.	Type of door readers required	Number of door readers will be
Scenario 4: Employees will use only their biometric for identification, without a tangible card/device	fingerprint reader	22
Next Step: Choose One		
<div style="display: flex; justify-content: space-around;"> Select Additional Scenario Use Only Primary Scenario Above Go to View Results Summary </div>		

Figure 5-4. Identification Scenario Selection Screen

Select Additional ID Scenario				
<p>There may be special areas that require an access control system different from the primary one defined above. In such cases, some employees may need an identification in addition to or instead of the primary type of ID selected above. In the space below, enter information as requested to describe the type of access needed for these special areas.</p>				
<p>Enter number of employees needing access to the special areas</p>		<input style="width: 50px;" type="text" value="15"/>	<p>For the employees needing access to the special areas will the ID will be in addition to, or instead of, the first ID defined above?</p>	
<p>Enter total number of doors requiring readers found at these special areas</p>		<input style="width: 50px;" type="text" value="3"/>	<p>Choose One</p> <p> <input checked="" type="radio"/> in addition to <input type="radio"/> instead of </p>	
<p>Would you like your employees to have a tangible card/device for identification? Note: if you answer "NO", the Scenario 4 - biometric only option is assumed, regardless of other entries below.</p> <p style="text-align: right;">yes ▼</p>				
<p>Would you like to use a biometric (fingerprint) to enhance verification of employees?</p> <p style="text-align: right;">yes ▼</p>				
<p>What type of sensor would you like to use to capture an employee's live biometric?</p> <p style="text-align: right;">public sensor ▼</p>				
<p>Where would you like to store an employee's reference biometric?</p> <p style="text-align: right;">on card/device ▼</p>				
<p>Where would you like biometric matching to occur? This is where the biometric comparison software resides. The matching compares the live biometric to the reference biometric at time of identity verification.</p> <p style="text-align: right;">on card/device ▼</p>				
<p>The additional ID scenario will apply for 15 employees.</p>			<p>Type of door readers required</p>	<p>Number of door readers will be</p>
<p>Scenario 3: Employees use a biometric encoded card for identity verification</p>			<p>card/fingerprint combo reader</p>	<p>3</p>

Summary of Your ID Scenario Selection(s)				
	Scenario	Number of Employees	Type of Door Readers	Number of Door Readers
Primary System	Scenario 4 biometric only with fingerprint reader - no card	380	Fingerprint Reader	19
Additional System	Scenario 3 biometric encoded card with fingerprint/card reader	15	Card/Fingerprint Combo Reader	3

Note: Employees under additional scenario have two forms of identification

Note: Number of door readers in the primary scenario added to the number in the additional scenario is the total number of door readers indicated on the Background Program Information sheet

Next Step	
Return to Map of Model	View Results Summary

Figure 5-4 (concluded). Identification Scenario Selection Screen

5.3.3 Results

The *Results* part of the model consists of two sheets reflecting different degrees of detail.

- The *Results Summary* sheet, as shown in Figure 5-5, provides a summary of total initial costs (hardware, software, installation, and training) and total recurring costs (maintenance), as well as initial and recurring costs for each of the five years in the life of the system. Costs may reflect a combination of the four identification scenario options.
- The *Detailed Cost Results* sheet contains unit costs for equipment. Resulting costs for specific pieces of hardware, software, other equipment, and other program costs - installation, training, and maintenance, and are further broken out with respect to each of the four identification scenario options. Results are given with respect to each of the five years in the life cycle. Some user input may be required for equipment unit costs, unless the user opts for the model supplied default values.

5.3.4 Additional Considerations

The *Additional Considerations* part of the model consists of four sheets that help the user assess potential benefits with respect to physical access, logical access, and access to services and privileges. For each of the various processes, the individual tasks required to complete each process are listed, along with time estimates to complete each task. These estimates are entered for each of the four identification scenarios.

- The first sheet in the set is *Enrollment Process*. Estimates are generated to reflect the time required to enroll employees and train them on the use of the identification card/device. These estimates are combined with *Cost of Resources* to generate cost of installation and training on the *Detailed Cost Results* sheet.
- The second sheet is *Performance: Physical Access*. Estimates are generated to reflect the time required to verify identity and grant or deny access to an employee at guarded and unguarded controlled access points. These estimates are generated for comparison across identification scenarios.
- The third sheet is *Performance: Logical Access*. Performance times across identification scenarios can not be directly compared for logical access. However, it is noted that the proof of concept device may be used for logical access without any additional hardware, as would be required for the other three identification scenarios. A few options for logical access are provided for comparison. Significant differences in time to access, or log on to, a computer are not expected. Sheet four is the
- *Performance: Specific Services* sheet. Estimates are generated to reflect the time required to perform a variety of services associated with well-defined operations – armory, evidence room, medical/pharmacy, guard tours, maintenance tours, roll call, and report preparation. Time to complete tasks associated with these operations are compared across identification scenarios. Time savings with respect to the proof-of-concept identification scenario, are converted to full-time-equivalent (FTE) and cost savings. It is noted that the benefits of any dollars, hours, and FTEs that may be saved may actually be best realized by re-incorporating these benefits into the program by providing additional time for employees, especially officers, to perform their intended jobs.

Cost Summary						
Instructions: Below is a summary of the initial and recurring five year costs associated with the identification scenarios you defined on prior sheets. There are no user inputs to this sheet. At the bottom of this sheet is a link to a detailed, itemization of each costs, by scenario.						
Costs	Year					Notes
	Initial	2	3	4	5	
Initial One-Time Costs						
Hardware: Identification Cards/Devices (see detail below)	\$75	\$8	\$8	\$8	\$9	
Hardware: Door Readers/Fingerprint Scanners (see detail below)	\$29,250	\$0	\$0	\$0	\$0	
Other Hardware	\$3,300	\$0	\$0	\$0	\$0	
Software: Products	\$0	\$0	\$0	\$0	\$0	enrollment software; required software
Other Software and Software Development	\$75,000	\$0	\$0	\$0	\$0	includes data migration; application development; optional software
Installation	\$24,136	\$2,414	\$2,586	\$2,867	\$3,290	
Training	\$8,542	\$838	\$898	\$995	\$1,142	
Other initial costs	\$0	\$0	\$0	\$0	\$0	includes additional security staff time and sw developer
Total Initial One-Time Costs	\$140,303	\$3,259	\$3,491	\$3,870	\$4,440	
Recurring Costs	Year					Notes
	Initial	2	3	4	5	
Maintenance: Hardware	\$1,631	\$1,689	\$1,809	\$2,007	\$2,303	includes hardware and software maintenance and software updates
Maintenance: Software	\$11,250	\$11,644	\$12,473	\$13,829	\$15,869	
Total Recurring Costs	\$12,881	\$13,332	\$14,282	\$15,836	\$18,172	
Cost Summary (concluded)						
	Year					Notes
	Initial	2	3	4	5	
Total Initial and Recurring Costs	\$153,184	\$16,592	\$17,774	\$19,706	\$22,612	
Ancillary Costs						other, indirect costs
Potential funds to offset costs	\$1,000					funds taken from Background Program Information sheet
Final Costs	\$152,184	\$16,592	\$17,774	\$19,706	\$22,612	
Total Final Costs Over Five Years	\$228,868					

Hardware Details	Quantity	Initial Costs
Hardware - IDs: Cards (no biometric)	0	\$0
Hardware - IDs: Card/Biometric Device	0	\$0
Hardware - IDs: Biometric encoded card	15	\$75
Hardware - IDs FYI: Number employees using biometric(s) only	380	\$0
Hardware - Readers: Card Readers Only	0	\$0
Hardware - Readers: Card Readers/Fingerprint Scanners	6	\$750
Hardware - Readers: Fingerprint Readers	19	\$28,500
	TBD	TBD

Next Step	
Return to Map of Model	Go to Detailed Cost Results

Figure 5-5. Results Summary Screen

5.4 Final Note

The model developed is intended to help the user assess a proposed access control program. The model may be tailored to a specific user's goals and operations. For example, the operations modeled as part of physical access and access to services are fairly general. If the user would like to model an operation not included in the model, or model an operation in a different way, this may be done in a couple of ways. The user may be able to define the background information or other input data to reflect this operation. Alternatively, the model may need to be modified by the original model developer.

6 Conclusions

The primary goals and objectives of this project were follows:

- Determine criminal justice entities and operations where positive identification of officers and staff is critical and where credentialing could improve operations related to identification, access control, and data management. Examine the resulting benefits to resource allocation and public safety.
- Develop a technology demonstration and proof of concept for selected criminal justice applications of credentialing using biometrics. Provide lessons learned and address the feasibility, reliability, and scalability of the concept.
- Provide guidance to criminal justice agencies for potential applications of the proof of concept into criminal justice processes and operations.

Conclusions have been reached in the following areas as a result of this project:

- **Biometric efficacy**

The use of biometrics in access control has the potential to improve security when compared with manual processing, speed throughput when compared with manual processing, and result in a more positive access control audit trail. That said, the agency issuing the BAC continues to have the responsibility of verifying breeder documents prior to issuance. This responsibility is greater when using a BAC since use of a biometric often implies a higher level of confidence in the identification.

- **Requirements and standards**

Requirements and standards for a BAC are needed for planning and implementation within a single program or agency. Additionally, for a BAC to be interoperable with other agencies or programs, common standards and requirements are critical. The requirements and standards must reflect the operational environment, as well as security threats and vulnerabilities.

- **Software development needed to support applications**

Realizing the full capability of BACs and access control systems requires some software application development. This software development provides smooth interfaces to an agency's or program's databases and systems, potentially increasing efficiency and simplifying operations. In some cases, particularly where proprietary software is involved, the vendor may be required to develop software applications. The use of products from vendors with proprietary software should be considered carefully, particularly with regard to the flexibility an agency may have to readily modify applications.

Independent source selections are critical in assessing technology options and vendor claims. Vendor offerings must be assessed with regard to planning, costs, reliability, functionality, and applicability to the agency's or program's operating environment.

- **Costs versus benefits**

Costs versus benefits of access control systems must be examined closely and should be reflected in an agency's strategic planning. Many benefits may be qualitative rather than quantitative. Occurrences of events that may threaten security, events that may be averted by some access control systems, may be very infrequent. Therefore, measuring the cost of infrequent, adverse events is often speculative. On the other hand, potential benefits and costs to day-to-day operations are more measurable and should be considered.

- **Implementation and interoperability**

Initial implementation of a BAC should be to well-defined operations with well-characterized populations. The individuals included in the population should have very specific roles, involving few individuals needing access to secure areas and to operations within a single jurisdiction. Subsequent implementations to larger populations within an agency can then follow once the issues and concerns associated with the initial implementation have been resolved. Extension to operations involving multiple jurisdictions, commonly using varied identification technologies, requires extensive coordination between jurisdictions. Sharing of access databases will be required in cross-agency and cross-jurisdiction scenarios so that the access level can be assessed for an individual by any jurisdiction. As always, for all implementations, a well-defined back-up system is necessary.

References

General Federal, State and Local Governments

1. Smartgov eStrategy
http://www.estrategy.gov/smartgov/whats_new.cfm#scbook
2. (Federal) Government Smart Card Handbook
<http://www.estrategy.gov/smartgov/information/smartcardhandbook.pdf>
3. Federal Identity and Credentialing Committee
<http://www.cio.gov/ficc>
4. *DoJ/FBI/DHS/IACP Endorse National Criminal Intelligence Sharing Plan, IACP Capitol Report*, Volume 3, Issue 10, May 21, 2004
<http://www.theiacp.org/documents/pdfs/CapitolReport/Newsletter052104%2Epdf>
5. Institute for Intergovernmental Research, *The National Criminal Intelligence Sharing Plan*, October 2003. Support by U.S. Department of Justice, Office of Justice Programs Award Number 2000-LD-BX-0003
http://www.iir.com/giwg/National_Criminal_Intelligence_Sharing_Plan.pdf
6. Department of Homeland Security Press Room, *DHS Launches US-VISIT Program Nationwide to Enhance Security, Facilitate Travel*, January 5, 2004, Contact Kimberly Weissman, Washington, DC
http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0332.xml
7. Schwarzhoff, Theresa, Jim Dray, John Wack, Eric Dalci, Alan Goldfine, and Michaela Iorga, *Government SmartCard Interoperability Specification – Version 2.1 Interagency Report 6887 – 2003 Edition*, National Institute of Standards and Technology, July 16, 2003
<http://csrc.nist.gov/publications/nistir/nistir-6887.pdf>
8. “EMS Insider”, Pentagon Response: Lessons Learned, May 2002
<http://www.jems.com/911/pdf/ins0502.pdf>
9. TSA, *TSA and The State Of Florida Team Up To Tighten Seaport Security*, March 18, 2004
<http://www.tsa.gov/public/display?theme=44&content=09000519800923a6>
10. Wait, Patience, *Great Expectation: Biometrics – Florida County Pioneers Biometrics*, Washingtontechnology.com, Vol. 18 No. 13, 09/29/03
http://www.washingtontechnology.com/news/18_13/cover-stories/21791-2.html
11. U.S. Congress, *Law Enforcement Officer Safety Act of 2004* (PL108-277 [HR 218])
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ277.108.pdf

Homeland Security Presidential Directive/ HSPD-12

12. Homeland Security Presidential Directive/ HSPD-12

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors, Issued by President Bush on August 27, 2004

<http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>

13. NIST – Personal Identity Verification (PIV) of Federal Employees/Contractors website

<http://csrc.nist.gov/piv-project/>

14. National Institute of standards and Technology (NIST) – Information Technology Laboratory – Computer Security Division, *Personal Identity Verification for Federal Employees and Contractors*, September 20, 2004

<http://csrc.nist.gov/piv-project/workshop-Oct072004/presentations/PIV-Opening.pdf>

<http://csrc.nist.gov/piv-project/Papers/PIV-BriefingSept16-2004.pdf> - September 16, 2004 version

15. NIST Draft Project Narrative - Personal Identity Verification for Federal Employees and Contractors

<http://csrc.nist.gov/piv-project/Papers/Narration-PIV-Briefing10-1.doc>

16. NIST PIV draft standard and supporting documents

<http://csrc.nist.gov/piv-project/fips201-support-docs.html>

Department of Defense Common Access Card (DoD CAC)

17. Dixon, Mary, DMDC presented to NIST, *Evolution of DoD CAC Program*, July 8, 2003

<http://csrc.nist.gov/card-technology/presentations/govt-requirements/Dixon-DOD-NISTv31.pdf>

18. Mestrovich, Michael Ph.D. (Federated Electronic Government Coalition), *Developing a Cross Certification Interoperability Proof of Concept and Pilot of Credentialing*, briefing, March 2003

<http://www.estrategy.gov/smartgov/information/MikeMestrovich111303.ppt>

19. Smart Card Alliance, Digital Security Initiative, *Department of Defense to Issue Up to 13 Million Common Access Cards for Smart-Card Enabled PKI*,

[http://www.smart.gov/library.cfm#category_d9c8061d-62b7-11d6-bcd1-](http://www.smart.gov/library.cfm#category_d9c8061d-62b7-11d6-bcd1-8aa2af114fbf)

[8aa2af114fbf](http://www.smart.gov/library.cfm#category_d9c8061d-62b7-11d6-bcd1-8aa2af114fbf) – Go to Case Studies subheading and click on *DoD Common Access Card* link

Transportation Worker Identification Credential (TWIC)

20. *TWIC Stakeholder Brief*

<http://www.tsa.gov/interweb/assetlibrary/TWICbrief25dec.pdf>

21. *Credentialing Project Technical Architecture* – Presented to Transportation Industry Association Stakeholders Meetings, April 11-29, 2002

http://www.tsa.gov/interweb/assetlibrary/Credentialing_Project_Technical_Architecture.pdf

22. *The Credentialing Program: Initial Questions and Answers and Definitions*

<http://www.aapa-ports.org/govrelations/TSA%20Credentialing%20FAQS.pdf>

23. Lazarick, Richard, *Biometrics in Aviation Security* – Presentation to 2004 NDIA, Homeland Security Symposium, May 27, 2004
http://www.dtic.mil/ndia/2004homeland/Lazarick_NDIA_05_27_04.ppt
24. TWIC Frequently Asked Questions
<http://www.tsa.gov/interweb/assetlibrary/TWICFAQs8-12-04.pdf>
25. TWIC
<http://www.tsa.gov/public/display?theme=68>

Corrections

26. Texas Instruments Press Releases 2003, *PIMA County Jail Upgrades Security With Texas Instruments 13.56 MHz RFID Tags, Cards and Readers*,
http://www.ti.com/tiris/docs/news/news_releases/2003/rel9-15-03b.shtml , September 15, 2003
27. M2SYS News and Events, *Wake County of Raleigh, North Carolina Selects M2SYS' e-Vigilance Biometrics System – Advanced Technology Verifies Inmate and Visitor Identities at County Detention Center Using Single Fingerprint Capture and Matching Process*, June 1, 2004
<http://www.m2sys.com/pr060104.htm>
28. Pinellas County, FL

Jackson, William, *Who's Who: Piece by puzzle piece, Fla. county checks suspects' identities*, Government Computer News, August 2, 2004, Volume 23, No. 21
http://www.gcn.com/23_21/tech-report/26755-1.html

Facial Recognition in Action, Government Security News, August, 2004, pp. 40-42
http://govtsecurity.com/mag/facial_recognition_action/
29. Boycott, Owen, *Top Security Jails Install Fingerprint Scan at Gates*, The Guardian – United Kingdom, August 5, 2004.
<http://www.guardian.co.uk/print/0,3858,4986152-103690,00.html>

Privaris, Inc.

30. Privaris, Inc.
<http://www.privaris.com/>
31. Privaris, Inc., BPID™ LFBT Security Device User Manual and Licensing Agreement, July 2004
32. Privaris, Inc. enrollment station manual
33. Privaris, Inc. API User's Guide v1.2.1, 8/16/04
34. Authentec, Inc. web site
<http://www.authentec.com/>
Note: Privaris, Inc. is the sole vendor of the technology for wireless and biometrics on-device authentication

Radio Frequency Identification (RFID)

35. RFID Journal
<http://www.rfidjournal.com>
36. Krim, Jonathan, *Embedding Their Hopes in RFID*, Washington Post, Business Section, June 23, 2004, pp. E1 and E5
<http://www.washingtonpost.com/wp-dyn/articles/A62061-2004Jun22.html>
37. Chen, Yen-Hung, *Getting Ready for RFID*, OR/MS Today, the Institute for Operations Research and the Management Sciences, June 2004, pp. 30-35

Card Readers

38. HID Compliance with government standards
HID Announces Support for U.S. Smart Card Interoperability Specification V2.1, BiometriTech News, July 21, 2004
<http://www.tmcnet.com/usubmit/2004/Jul/1058680.htm>

Biometrics

39. Wayman, James L., *Biometric Identification Standards Research, Final Report, Volume One, Revision 2*, December 1997, College of Engineering, San Jose State University, prepared under FHWA CONTRACT DTFH61-95-C-00165
40. Blackburn, Duane M., March 2004, *Biometrics 101, Version 3.1*, Federal Bureau of Investigation
http://www.biometricscatalog.org/biometrics/biometrics_101.pdf
41. Phillips, P. Jonathon, Alvin Martin, C. L. Wilson, and Mark Przybocki, *An Introduction to Evaluating Biometric Systems*, IEEE Computer Magazine, February 2000, pp. 56-63
<http://www.frvt.org/DLs/FERET7.pdf>
42. InterNational Committee for Information Technology Standards (INCITS) M1 biometric standards group
http://www.incits.org/tc_home/m1.htm
43. International Standards Organization (ISO) biometric standards group JTC1-SC37
<http://www.iso.ch/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=5537>

Card Technology

44. Magnetic stripe -125 bytes capacity
<http://www.info.gov.hk/digital21/eng/knowledge/smarttech.html>
45. Smart cards - one thousand to 64K bytes capacity
<http://www.info.gov.hk/digital21/eng/knowledge/smarttech.html>
46. Optical memory card - up to 2.8 Megabytes capacity
<http://csrc.nist.gov/publications/nistir/IR-7056/Capabilities/Price-optical.pdf>

General Access Control

47. Prepared by RTI for NIST, *The Economic Impact of Role Based Access Control*, Planning Report 02-01, March 2002
<http://www.nist.gov/director/prog-ofc/report02-1.pdf>

Commercial Applications

48. Pero, Jennifer, *Access Control Takes Center State at the Academy Awards*, February 1, 2003
http://www.ti.com/tiris/docs/news/in_the_news/2003/2-1-03.shtml
ID card worn around the neck; Texas Instrument's RFID technology
49. Hall, Steve, *World Bank Employs an Integrated Security System to Protect Its Employees and Properties in Washington, DC*, Government Video Magazine,
http://www.swhouse.com/pdfs/World_Bank.pdf

Appendix A Biometrics and Corrections

The concept of Biometric Identification is widely known and used in the corrections community. Almost every Corrections facility already fingerprints inmates and sends the fingerprints onward into the Criminal Justice system for positive identification and feedback on the individual's background. However the fingerprint capture is usually a manual process involving ink and fingerprint cards, and positive identification can take days or weeks after submission to state or federal fingerprint database systems.

While the use of *automated* Biometric Technology already has been applied in some locations in the Corrections community, such technology usage has been limited to a relatively small number of applications and sites throughout the United States. The limitations are primarily due to the limited technology available, the small number of biometric technology vendors, the lack of widely available information about biometric technology and the fragmented nature of the Corrections Market.

This appendix contains a table of some existing uses of automated biometric technology in the Corrections community. The use of automated biometrics technology has already been demonstrated at several Corrections sites in the US. The most notable uses are in county jails at different locations and using different biometric data and sensors. While different biometric sensor technology is used in the biometric data collections, the underlying demographic data storage, retrieval and display concepts are similar.

Table A-1. Summary of Biometrics in Correctional Facilities

Biometrics in Correctional Facilities - Summary							
Agency	County	State	Program Objective	Volume	Technologies Being Employed	System or Operations Being Replaced	Notes
JAILS							
Jefferson County Sheriff's Dept	Jefferson	AL	Inmate and Visitor ID; check aliases and outstanding warrants; photos searchable from patrol car	1,300 beds; 25,000/yr	facial recognition		1
Pima County Sheriff	Pima	AZ	Inmate ID & movement	1600 daily/124+ readers	RFID wristband	manual ID	2
Pima County Sheriff	Pima	AZ	Officer ID & movement	300 daily/124+ readers	RFID badges	manual ID	2
Los Angeles County Sheriff	Los Angeles	CA	Mug Shot Search		Facial ID		3
Los Angeles County Sheriff	Los Angeles	CA	Inmate ID		RFID & Fingerprint		3
Jefferson County Sheriff	Jefferson	CO	Inmate & Employee ID	17,000-19000/yr	Iris Scan	manual ID	1
Sarasota County Sheriff	Sarasota	FL	Inmate ID		Iris Scan		4
Pinellas County Sheriff	Pinellas	FL	Inmate & Visitor ID		Facial recognition (Viisage)	manual ID	5
Cobb County Sheriff	Cobb	GA	Inmate ID and alias check	2,500 beds	1:1 facial recognition (Geometrix)		6
Cook County Sheriff	Cook	IL	Inmate ID		Retina Scan		7
Barnstable County	Barnstable	MA	Inmate ID		Iris Scan		8
Prince George's County Dept of Corrections	Prince Georges	MD	Employee ID		Facial recognition		9
Wake County Sheriff	Wake	NC	Inmate & Visitor ID		fingerprint + digital photo	manual ID	10
Bergen County Sheriff	Bergen	NJ	Inmate ID	8000/yr	Iris Scan	ID bracelet/fingerprint	11
Lancaster PA Sheriff	Lancaster	PA	Inmate ID		Iris Scan		12
USN Consolidated Brig	NS Charleston	SC	Employee & Inmate ID & Access		Fingerprint	Facial & Eye Scan	13
PRISONS							
California Dept of Corrections	multiple sites	CA	Employee ID, Access & Safety	49,000+	Fingerprint ID & Bar Code Badges	manual ID	14
California Dept of Corrections	multiple sites	CA	Inmate ID & Movement	155,000+	Fingerprint ID	manual ID	14
State of Hawaii	multiple sites	HI	Inmate ID & Movement	5,500 inmates			15
Minnesota Dept of Corrections	multiple sites	MN	Employee ID & Access	4000 users	fingerprint ID	manual ID	16
PA Dept of Corrections	multiple sites	PA	Employee ID & Access	1200 users	fingerprint ID+ photo comparison	manual ID	17
Washington State Dept of Corrections	multiple sites	WA	Parolee ID & Reporting	70 kiosks, 26,000ID/mo	IR Hand Geometry	manual ID	18
Wisconsin Dept of Corrections	multiple sites	WI	Employee, Visitor & Inmate ID	100,000/ yr	facial recognition & smartcard	manual ID	19
NOTES							
1. There are more than 70 federal prisons, 900 state prisons, and 3200 jails in the United States.							

Sources for Table: Biometrics in Correctional Facilities

1. Jefferson County, AL
findBIOMETRICS.com, *Viisage Awarded Contract with Jefferson County, Alabama to Aid in Criminal Identification* - June 28, 2004
<http://www.findbiometrics.com/viewnews.php?id=1263>
2. Pima County, AZ
ContactlessNews.com, *Pima County Jail Upgrades Security With Texas Instruments 13.56 MHz RFID Tags, Cards and Readers*, Thursday, September 18 2003
<http://www.contactlessnews.com/news/2003/09/18/pima-county-jail-upgrades-security-with-texas-instruments-1356-mhz-rfid-tags-cards-and-readers/>
and
TI.com, *Pima County Jail Upgrades Security With Texas Instruments 13.56 MHz RFID Tags, Cards and Readers*, Thursday, September 18 2003
http://www.ti.com/tiris/docs/news/news_releases/2003/rel9-15-03b.shtml
3. Los Angeles County, CA
Jarvis, Angela, Forensic-Evidence.com, *Are Privacy Rights of Citizens Being Eroded Wholesale?*, no date provided.
<http://www.forensic-evidence.com/site/ID/facialrecog.html>

By News Story, Government Technology, *Government's Partners*, September 29, 2003
<http://www.govtech.net/?pg=news/news&id=2003.09.29-70007>

Dean, Joshua, CNN.com, *Automated Fingerprinting Comes of Age*, September 9, 1999.
<http://www.cnn.com/TECH/computing/9909/09/auto.id.idg/>

Justice Technology Information Network, August 12, 2004
<http://www.nlectc.org/justnetnews/08122004.html>
4. Sarasota County, FL
Justice Technology Information Network, October 21, 1999
<http://www.nlectc.org/justnetnews/10211999.html>

Coleman, Stephen, *Biometrics in Law Enforcement and Crime Prevention – A Report to the Minnesota Legislature*, April 1999
<http://www.metrostate.edu/slc/pdf/biometrics.pdf>
5. Pinellas County, FL
Whitaker, Aja, Tampa Bay Business Journal, *Pinellas County Jail adopts high-tech management system*, August 6, 2004
<http://www.bizjournals.com/tampabay/stories/2004/08/09/story8.html>
6. Cobb County, GA
Drudge Report, August 18, 2004, *Facial Recognition Systems Successful at Cobb county Adult Detention Facility*
http://www.drudgereportarchives.com/data/2004/08/18/20040818_185603_flash5.htm

7. Cook County, IL
Estep, Bill, *Perspectives: For the Record*, a publication of Ohio University,
Spring/Summer 1998
<http://www.ohiou.edu/perspectives/9801t/tech2.htm>
8. Barnstable, MA
National Center for State Courts – Court Technology Lab – Biometrics Home –
Individual Biometrics - Iris Scan
<http://ctl.ncsc.dni.us/biomet%20web/BMIris.html>
<http://www.ncsconline.org/>
9. Prince George's County, MD
2002 PRIMEDIA Business Magazines and Media, Access Control and Security
Systems Integration, *Face Recognition On the Job*, March 1, 2002
http://securitysolutions.com/mag/security_face_recognition_job/
TechBeat, National Law Enforcement and Corrections Technology Center, *Counting
On Biometrics*, Winter 2003
<http://www.nlectc.org/txtfiles/tbwinter2003.html>
10. Wake County, NC
PRNewsWire, Fox Carolina, *Wake County of Raleigh, North Carolina, Selects
M2SYS' e-Vigilance™ Biometrics System*, June 8, 2004
<http://www.fox21.com/Global/story.asp?S=1925474>
11. Bergen County, NJ
Conference Announcement -Advanced Learning Institute
<http://www.aliconferences.com/conferences/biometricssummit/main.html>
http://onclick.blogs.com/biometrics/industry_news/
12. Lancaster, PA
Bourque, Lyne, InsideID, Keeping an Eye on Secure Access: Iridian Iris Scan, April
14, 2004
http://www.insideid.com/id_management/article.php/11781_3346651_1
13. USN Consolidated Brig
Associated Press, TheState.com, *Navy Brig Testing Biometric Tracking*, December 1, 2003
<http://www.thestate.com/mld/thestate/news/local/7387587.htm>
14. California Department of Corrections
findBIOMETRICS.com, Identix Receives Certification from California Department
of Justice For TouchPrint Pro Full Hand Scanner, March 4, 2003
http://www.findbiometrics.com/Pages/news_releases/news321.html
15. Hawaii
findBIOMETRICS.com, Biometric Corrections Management System Installed for
State of Hawaii
http://www.findbiometrics.com/Pages/law_articles/law_4.html

16. Minnesota Department of Corrections
findBIOMETRICS.com, Minnesota Department of Corrections Purchases 3,000 User License of Saflink's SAFmodule for NMAS SAFLINK; Biometric Solution to Enhance Security of DOC Facilities; Rollout Under Way, December 31, 2002
http://www.findbiometrics.com/Pages/news_releases/archives/news232.html
17. Pennsylvania Department of Corrections
Advanced Network Systems Concept Center, *COMMONWEALTH OF PENNSYLVANIA: Biometric technologies boost prison security*
<http://www.csc-ansc.com/stories/biometrics.asp>
18. Washington State Department of Corrections
Kiplinger.com, 2004 CMP Media LLC, *10 Technologies State Governments Are Buying -- Integrators and vendors help states streamline processes and meet legislative mandates*, Source: VarBusiness
<http://www.kiplinger.com/print.php>
19. Wisconsin Department of Corrections
1999PRNewswire/ -- Viisage Technology, Inc, *Viisage Selects Eltron P500 Card Printer for Wisconsin Department Of Corrections Project*, October 7
<http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=105&STORY=/www/story/10-07-1999/0001038909>

Appendix B Corrections Operations

As part of this project, Mitretek staff visited the Arlington County Sheriff's office and toured the court and the jail facilities with senior sheriff's deputies. The facility is one of the more technically advanced Direct Supervision facilities in the country. The facility has a non-jail like appearance which effectively camouflages the operations amid a highly urban downtown area.

The Arlington County Detention staff manage more than 500 inmates daily. The 200 staff members consist of more than 150 Correctional Staff plus administrative support personnel. The Correctional Staff are Certified as Virginia State Law Enforcement Officers and are responsible for the movement of inmates within the facility.

The purpose of our visit was to learn about operations in the facility and to document existing procedures. The main areas of our focus were intake, the housing pod, and visitation.

Prisoner Intake Process

Prisoners arrive at the Jail facility via police, sheriff, or other law enforcement agency to include federal authorities. Most will enter the facility by way of the garage where officials begin the intake process. The garage is automatically controlled to secure a vehicle inside the building before the door is lowered. Once the door is securely down, the prisoner(s) is(are) taken from the vehicle into the intake processing area. The prisoners are processed while in the holding/intake area. They are fingerprinted, photographed, searched, and asked appropriate identification questions.

Jail staff make a decision as to the length of stay the prisoner is likely to receive. If the prisoner is being booked on a misdemeanor or lesser offense, they will likely be released within 24 hours. In that case, the prisoner will be held in a different area within the intake perimeter, but they will be processed in the same manner. A prisoner being processed into the facility on a more long term stay basis will be taken to a different holding area while the appropriate commitment documentation is collected. Once the prisoner's information is up to date, they will be taken into the jail facility and assigned a housing pod in the initial holding area. Separate areas are available for violent prisoners, handicapped or injured prisoners and psychiatric evaluations.

After the prisoners are placed in the initial pod area, the prisoners are classified for assignment to a long term housing pod. The classification process assesses the inmate's potential behavior and expected conduct while in the jail. Based on the assessment prisoners are assigned to a housing pod with like classified inmates. The degree of inmate supervision by corrections staff in the pod varies by classification.

At this time, the intake process includes obtaining a single inked fingerprint on the file jacket for identification purposes. The print is used for comparison at release to assure correct prisoner identification. No automated means of prisoner identification is available at the intake point and fingerprint comparison must be performed manually. Since there are no magnifying devices available for print comparison and deputies are not trained

fingerprint specialists, deputies also asked prisoners questions about personal data kept in the prisoner's file. Figure B-1 depicts the Prisoner Intake Process.

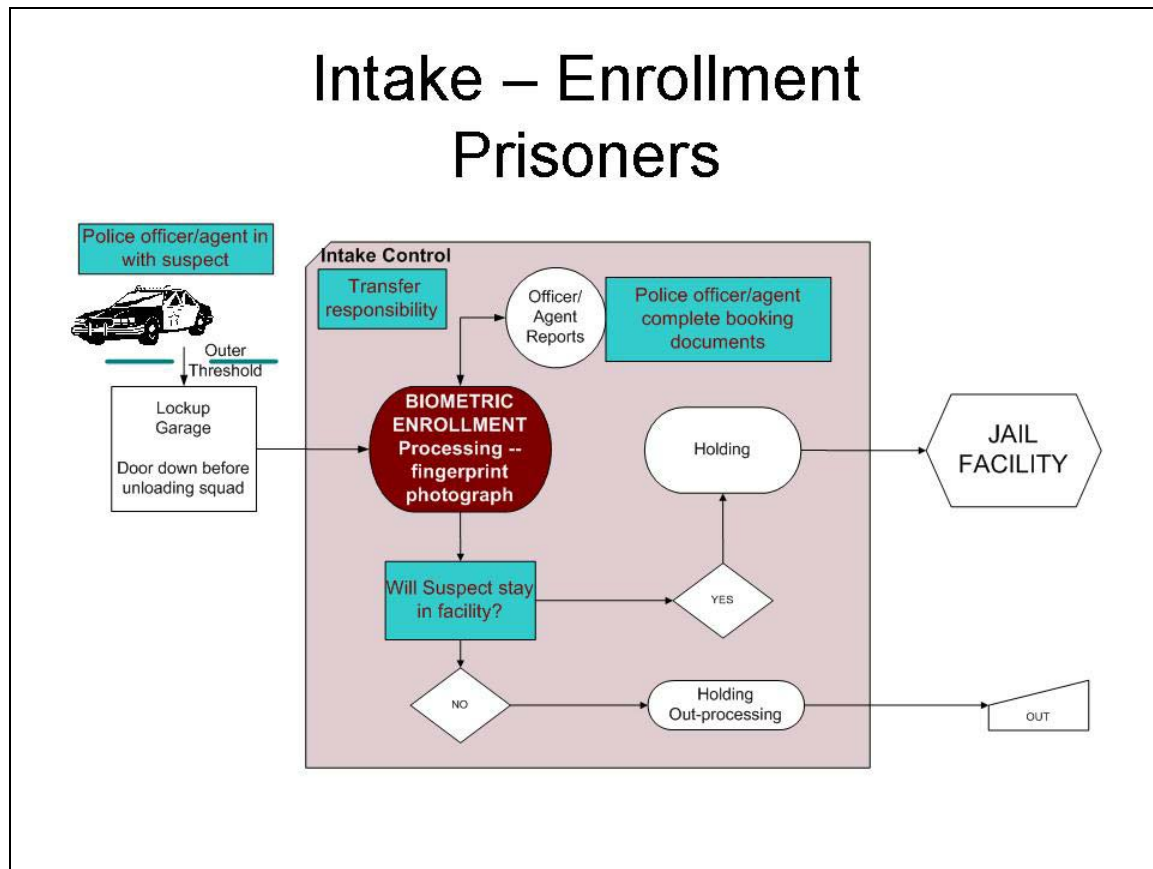


Figure B-1. Prisoner Intake Process

Intake Problems

The intake module of the jail appeared to flow smoothly and maintain adequate control. The issue that seemed troublesome for staff was positive inmate identification, in particular, knowing the correct inmate has been released. Reducing the potential for releasing the wrong individual.

The intake process currently uses a single finger print as verification and identification upon prisoner release. Staff, however, warned that the procedure for checking and verifying this print was not closely followed. As a result, the risk for improper release of an individual was higher than tolerable.

Potential for Improvement Through Biometrics

Biometric devices today are easier to use than ever before. Enrollment is quick and reliability excellent. The intake process in the jail is rigid, each inmate going through a standard of processes such as routine photographs, fingerprints, questions, identification tagging, etc. Inserting biometric enrollment would be unobtrusive and provide a higher standard of verification and validation within the system.

Once the inmate is biometrically enrolled at entry, policy and procedure followed at exit could and should assure near fail-safe positive identification. The decision to store the biometric in a database or in the device can be made by the individual institution. If the biometric is stored in a central repository, it can be accessed within the correctional or jail setting and compared to visitors or other individuals attempting to falsely identify themselves.

Inmate Residence Pod

As illustrated in Figure B-2, the inmate residence pod in the Arlington County Jail is an area in which all inmate living activity takes place. The open area in the center holds several tables and offers inmates an area in which to congregate, meet, and otherwise conduct passive activities. Around the two level outside rim of the pod other rooms consist of sleeping areas, laundry, activity rooms, and bathrooms with showers.

The Corrections Officer (CO) is located on the main floor where they maintain a full view of the pod. All activities are monitored and behavior documented. The CO is responsible for maintaining control in their pod. They have specialized training to handle control problems.

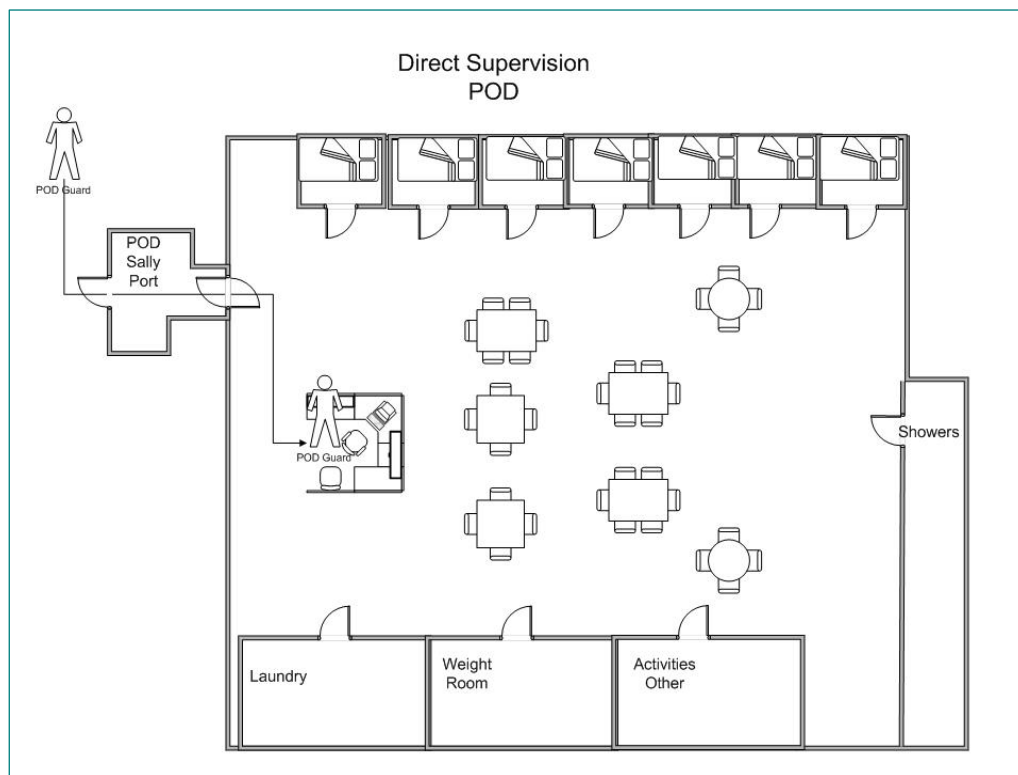


Figure B-2. Illustration of an Inmate Residence Pod

POD ACTIVITIES

The Pod Activities graphic in Figure B-3 depicts sequential activities at entry to a pod and denotes simultaneous activities and tasks in the pod.

The tasks described below describe functions and processes related to a correctional officer working within a medium security direct supervision pod.

Arrival

Upon arrival at the facility, an officer will first check in and be authorized to enter. They will then obtain the required equipment for work on the pod. This may include, but will not be limited to cuffs, flashlight, first aid gear, body alarm (if tipped, or cord pulled, will send an alarm to central control). Often, officers will be asked to attend a roll call at which time they will be briefed on prior events in the facility and pods. Information pertaining to prisoners, events that took place, upcoming activities, and other information specific to the shift will be disseminated at roll call.

The officer then enters the sally port of their assigned pod where they identify themselves to the officer on duty. They will enter the pod and be debriefed by the on-duty officer and accept transfer of authority. The officer will conduct a tour of the pod where they will re-establish inmate contact and establish a new contact with inmates who have arrived since their last tour.

During a pod tour, depending on the facility, the officer may be required to use some type of electronic system to record movement and checks made at prescribed points of control within the pod. For example, an officer may be required to conduct pod rounds periodically. While on these rounds, an electronic device such as an RFID tag or card may be used to swipe or pass by an electronic pad. As the officer passes these points, he passes his tag in front of a reader. The reader then sends a message to a data system that in turn records the officer's identification, his location and the time and date he passed the point of reference. The tag carried by the officer may contain personal identification and biometric authentication for certainty.

In-Pod Tasks

Once the officer is inside the pod, they will remain there throughout their tour of duty unless appropriately relieved by another officer or authority. While inside the pod, the officer must monitor inmate activity and maintain control. The list of activities below is also depicted in the Pod Activities graphic.

- Periodically, throughout the shift allow visitors (parole agents, tours, prison employees) to enter the pod and speak to inmates.
- Prepare the inmates for transportation outside the pod for visiting, attending court, or meeting with attorneys.
- Oversee various pod work details, e.g., cleaning.
- Prepare the inmates for meals—allow inmate workers onto the pod to distribute food; assign inmates to clean up after the meal.
- Collect requests from the inmates to see their attorneys, parole officers, judges, etc., and to process commissary accounts.
- Allow medical staff to enter the pod to dispense medications—oversee the process to make sure it runs efficiently.

- If an inmate acts out, officers contact central control which then dispatches floor support personnel to quell the disturbance. The pod officer is instructed to NOT get directly involved in any use of force (he/she may after all, still be assigned to work with these people at a later time). The pod officer's first duties are to request floor support and lock all the inmates in their cells.
- For minor infractions, pod COs can mete out punishment to an inmate such as locking them in their cell for a period of time, turning off the TV, etc.
- Off the pod, COs might be involved in testifying at disciplinary hearings, attending training, etc.
- Monitor laundry activities based on assigned times.

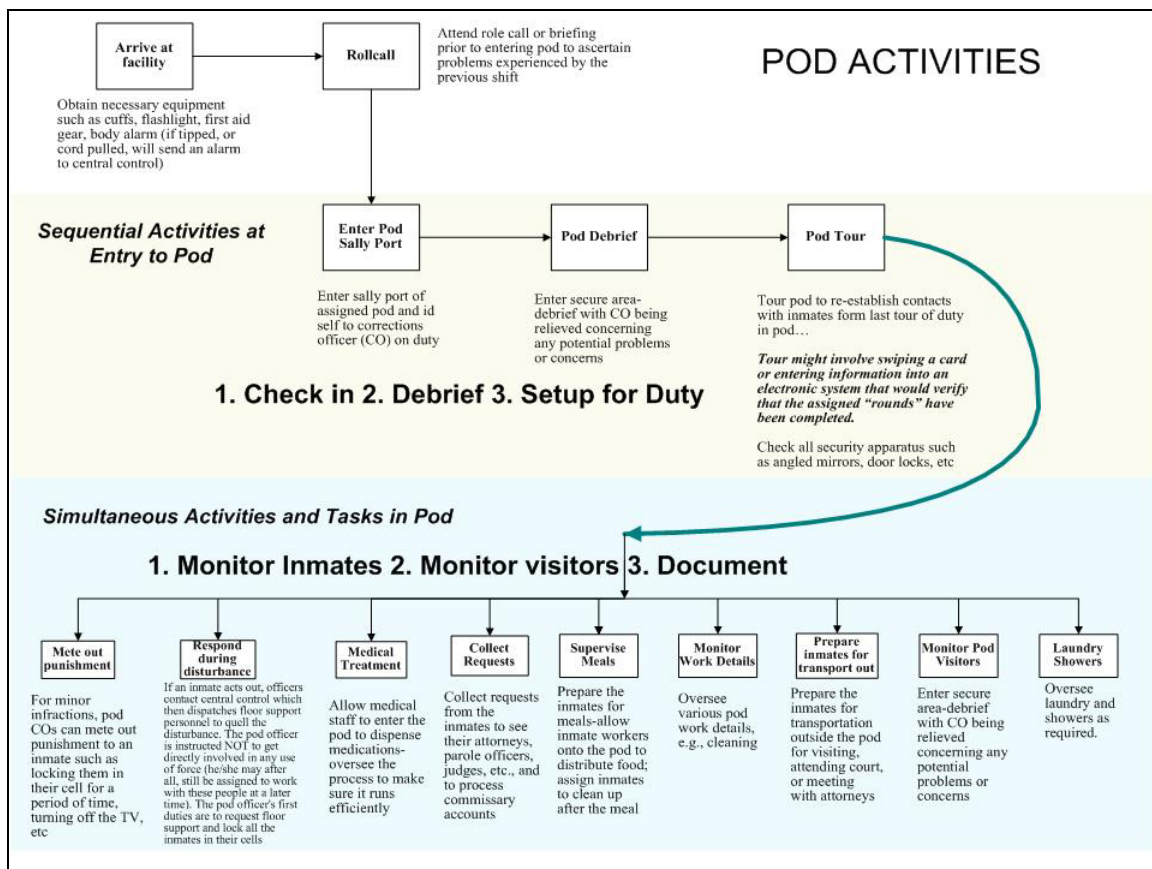


Figure B-3. Pod Activities

Pod Activity Problems

The CO is split among the many tasks they must do simultaneously. In addition to assuring pod control and smooth operation, the CO must also document activities and keep a log of events occurring within the pod. The nature of pod life creates difficulties in documenting it efficiently and accurately.

In the event of a threat or disturbance in the pod, the CO is expected to lock-down the area as quickly as possible, gain control when possible, and then assure the event is

properly recorded. Often, situations result in the introduction of additional staff to the pod. The situation can become chaotic and even deadly. Such activities and events require accurate documentation.

When the CO is required to record an event or task, their attention is taken away from the pod itself offering, however short, a moment in which the inmates are not being monitored. The time required for the CO to document tasks and events is dependent on the nature of the task or event. At times, the time period required for documentation can compromise the secure setting of the pod.

Potential for Improvements Through Biometrics

Biometrics is a way to authenticate a device, which in turn is associated with the individual. Using a biometric as a way of verifying identity, it can greatly enhance confidence and shorten the authentication process.

Documentation in the pod is usually a check-off type list of performed tasks or conducted rounds. Each time the officer passes a room, checks on an inmates activity in one of the adjacent rooms, or opens or closes doors, a “check” of some type is made to record the task. Using a biometrics device, the “check-off” can be performed more accurately.

Each task deemed appropriate to biometric use, i.e. door manipulation, can be set to record information appropriate to the given task. For example, if a CO is required to check rooms at a prescribed time, instead of keeping track of each room, writing each time they went by, they would simply use a biometrically controlled device to “trip” some type of control that would in turn automatically document the date, time, the officers credentials, the room or area of activation and could provide prescribed notes to be recorded in a database. The officer would never need to take time away from their main duties, pod control, to document routine tasks. If necessary, a running printout or running onscreen log could be generated. In addition, those tasks deemed routine, but critical to operations, would more accurately and efficiently be recorded into a data system. The data would also be available for historic querying and for further analysis of pod and jail activities.

During a disturbance or emergency, many tasks cued up in procedures could be automatically recorded, such as locking doors, checking activity rooms, summoning additional help, and/or entering and exiting staff. The CO would not need to estimate times and movements, all activities associated with the biometric could be controlled and documented with the swipe of a device or movement past a particular transmitter/receiver.

The use of biometrics in the pod area could:

- Improve time management by removing the need to hand document many tasks;
- Provide improved accuracy in task and event documentation;
- Move focus of CO from documentation to pod control;

- Provide additional officer safety options by offering a special option in the biometric device that would issue an alarm or signal when activated, or an offer an “officer down” indicator.

Visitation

Figure B-4 illustrates a jail visitation schema. The process for visitor identification is critical. All visitors must be identified and processed. When the visitor arrives at the jail facility, they are met by jail personnel who will use photographic identification cards to verify identity of the individual and to associate the visitor to a prisoner. Identity of the visitor is critical to making decisions about the nature of the visit and the location of the visitation. Each record is processed and stored for future visits. The database containing visitor information also can be an important tool for investigators.

All jail visits pass through a central entry point where they are assessed by type of visitor. Visits are generally categorized into legal and other. In all cases, jail officials contact the prisoner via pod staff to assure they are brought to the visiting area assigned. In most cases, the visitor is allowed to enter the assigned visitation area after the prisoner is in; however, this is not always the case. In some instances, the visitor enters the assigned area first. In all cases, the visitor’s and the prisoner’s movements within the visitation area are controlled by jail staff.

Legal visits are private. In those situations, the prisoner is taken to a private room or location in which they may have unrestricted contact to their representative. Legal visits are isolated from other types of prisoner contacts.

Personal or other types of visits, such as clergy, may be in a public area or they may be private as deemed appropriate by jail officials.

Problems with Visitation

Several problems are inherent in corrections or jail visitations. First, many visitors were once inmates. Some are currently on probation or parole and must be monitored at all times. Others use a jail visit to continue their criminal behavior, but identification of these individuals is often lost within the visitation process. Second, identifying repeat visitors can be impossible, especially if the day is busy and many people are awaiting access. Many repeat visitors are also repeat offenders. Third, visitation is done onsite, therefore, control of the visitor population is critical to institution stability. Sure identification and swift movement through the visitation process is vital.

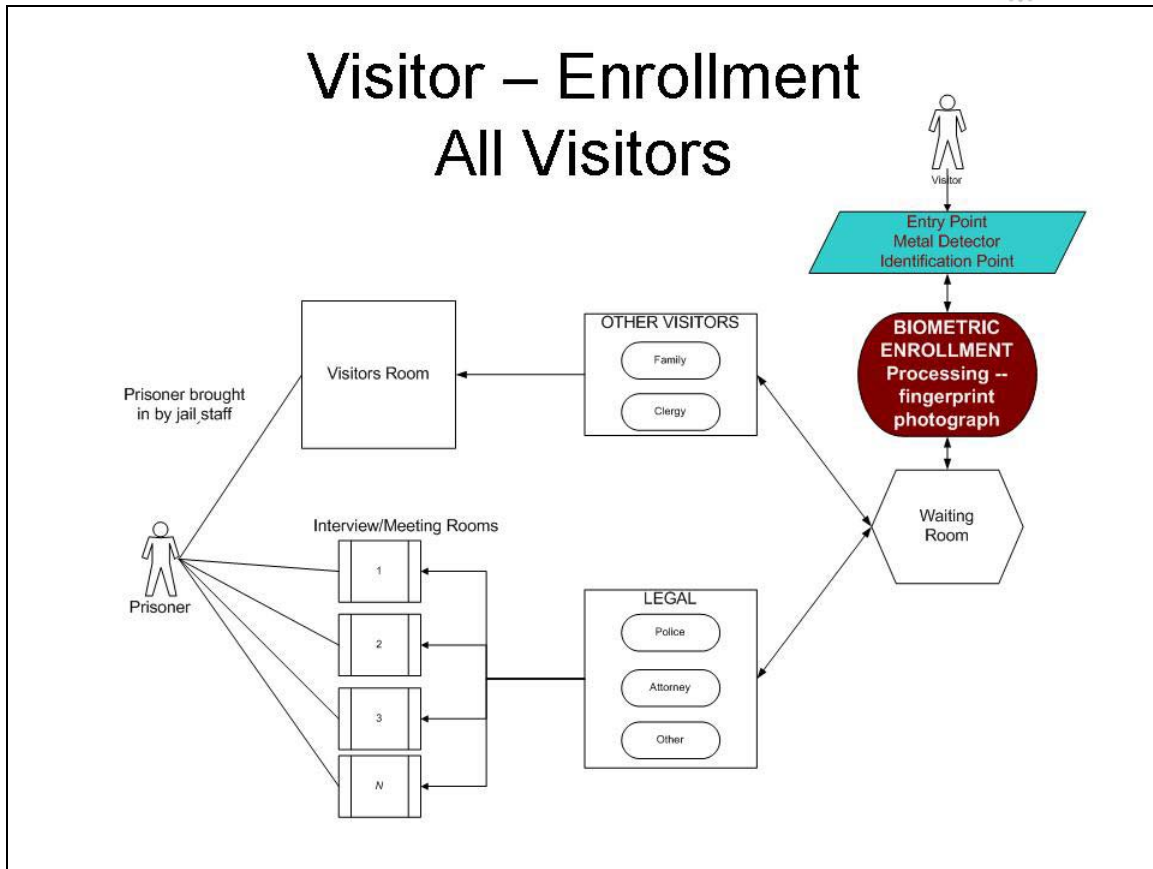


Figure B-4. Visitation

Potential for Improvements Through Biometrics

Recording visitations, identifying individuals and moving the process along are important to the visitation module of a correctional institution or jail. Using a biometric at this junction could:

- Improve the speed of processing;
- More positively identify individuals;
- Provide an historical record of visits;
- Prevent false identification.

Data obtained at the point of visitation is a rich source of information that can be used as analysis to better understand patterns and movements of inmates and their associates. Visitation data is also a good source for criminal investigators attempting to track a known suspect.

Appendix C Application of the Proof of Concept to the Inmate Population

Consider the operation where each suspect is enrolled on a Privaris device. Once biometrically enrolled, the suspect can be processed in and out of the jail facility quickly or they can be brought in for a longer period of time. Regardless of the length of stay in the jail facility, the biometric device will stay with the suspect or inmate and can be used as identification verification at any point in the booking, day-to-day living, or exit procedures. The biometrically based keychain provides to jail staff the added assurance that the individual before them is positively identified.

The keychain can be programmed with an array of credentials thereby assuring identification and reducing the likelihood of a false prisoner release or a misidentification during routine jail processing. The device is unobtrusive and can be made the responsibility of the inmate, the COs, or the pod guards while the inmate is physically inside the pod. There is a need to be able to visually distinguish devices among device owners, since all devices look alike. Distinguishing feature should allow for re-issuance of devices by overwriting credentials when inmate is released and device is assigned to a new inmate.

As the prisoner moves from station to station through out the facility, they should be asked to pass their device in front of access points where their credentials are verified. The need for guards to be constantly logging movement of prisoners is greatly lessened as they will be digitally recorded at each passing. Additionally, Geographic Positioning System (GPS) capability would allow for tracking of all movement.

Upon exiting the facility, the inmate should be required to authorize their identity for the final time. The system should note the prisoner's location, document that they are in exit processing, and record that they were positively identified and released.

The keychain biometric device may also be used for jail staff. Easy to use, convenient and pocket-sized, the staff member can use the device to key in and out anywhere in the facility. The assurance of identity lessens the need for constant monitoring of those entering and exiting. It allows jail monitors to spend their time more effectively monitoring situations and jail activities and less time opening and closing doors.

Example

A suspect is arrested and brought into the jail for booking. The suspect is processed following current intake steps. However, the jail staff adds to the process a short and simple enrollment for the keychain biometric. Four different fingers are used for the suspects biometric, their photograph and personal data are programmed into the device. The device is then given to the inmate and may be tagged onto their clothing or given to them to hold in their pocket. The jail staff explains to the prisoner the importance of maintaining control of the keychain and that part of their responsibility while in the facility is control of the keychain.

For the sake of this example, we will assume the prisoner is wearing prison garb that has on it a permanent or locked keychain. It can be extended on a retractable cord so the prisoner can pull the keychain out to pass it by access points, but it is retracted to the inmate's body after passing the device. It will act much like an employee identification card worn on a lanyard with a retractable cord.

The prisoner's information is keyed into the jail system and ultimately coded into access points throughout the facility. The prisoner is then moved to the pod where they will be housed until such time as the court orders their release. As they move into the pod, the prisoner is asked to pass their keychain in front of the access point and they are positively identified (as is the staff member) which prompts the door to unbolt. Both move into the pod.

While the prisoner is in their cell and have taken off their jail garb, the device will still be within their control. Whenever they exit the cell, they will pass the device in front of an access point that tells the pod guard they have left their cell. The guard may be alerted on an electronic board showing movement and location of all prisoners or they may simply see the movement as they watch the pod area. The device will also be used to enter any other areas currently monitored by other types of logging, such as showers or recreation areas. The prisoner will pass their device in front of access points and if they have been given access to the area and they are allowed in that area during the time they are attempting entry, the doors will open and the movement logged. Our example inmate has used the showers and the recreation area. All of their movement has been logged digitally.

Our prisoner has also been given rights to the visitation area. On a particular day, they receive a visit from a family member. Notification of the visitor is made to the pod guard who in turn notifies our prisoner. They are give permission to move to the visitation area and do so by using their device to key in and out of all access points. They may or may not be escorted by a jail staff member, depending on the particular jail layout. Upon their return, the prisoner keys back in using the biometric device and their movement, time of visit, and visitor information are all recorded. The prisoner then goes about their daily routine in the pod area until they retire for the night.

Visitor information is also recorded in the system as the biometric device is also used to positively identify visitors. Each visitor arriving at the jail facility are told that their visit depends on positive identification of who they are. They are enrolled in the keychain program and added to the database. But more importantly, they are associated to the prisoner(s) they visit. Once enrolled, subsequent visits are easier.

The next day our example prisoner is required to appear in court. They again are asked to key in and out of all access points between the jail and the courtroom. Their movements are recorded digitally, providing a movement-by-movement record. Times are also shown as the prisoner moves through the facility and into the courtroom. Although, in this case, escorted by prison staff, the verification and validation of movements through the

positive identification of the biometric greatly reduces error and offers a substantiating log of activities.

In addition to substantiating movements through logging, the use of the device and its subsequent digital recordings can be used at a later date to analyze jail movement. With information about staff and prisoner activities and movement throughout the facility, executives tasked with facility control and maintenance can better target problem areas or identify hot spots of activity otherwise unknown. The digital record can be kept indefinitely or for a specified period of time. Analysis on facility movements can be done periodically to better understand jail dynamics. A rolling thirteen month historical accumulation of movement could indicate seasonal swings in activity or it may indicate certain bottlenecks in the facility. Attempts to correct troublesome areas could be monitored and deemed successful or not successful based on continued analysis of historical data.

Our example prisoner moved through a problem area along their route to the courthouse. Their keychain biometric device triggered an access point that allowed them to pass along their course, but it triggered a deviation alert to analysts who have been watching movement through the corridor. With the alert triggered, executive management will have substantiating documentation to make a change. The information provided them will set in motion a process change request for jail management strategists.

Upon completing the courtroom appearance, our example prisoner is escorted back to the pod. He keys in at all the access points on his way back to his cell. The Judge ordered his release, so they are processed out according to jail protocol, but in this case, their out processing is also recorded step-by-step as they move from pod to corridor back to booking and out.

The most critical point of the jail processing is verification and validation that the inmate being released is the correct individual. Until now, this has required human intervention and at times has been cause for concern. Using the biometric keychain and new jail policy requiring the final checkout to include verification through a last access point, assurance of identity is greatly improved. Our prisoner keys in at the out processing access point and on the jail staff's computer screen, their biometric is verified along with their photograph. Not only does the jail staff see the photograph, but they also see that the biometric of the individual standing before them has assured them of their identity. Our prisoner is released safely.

It is well known that perpetrators return to jail facilities with some degree of regularity. Our example prisoner is no exception and later in the year they are arrested again for a similar offense. When brought back into the jail, the biometric and other credentialing is already in the system and a positive verification is made on the spot. The cycle begins again.

Appendix D Application of the Proof of Concept to Critical Incident Management

This appendix uses a crime scene as an example of extending the concept to a more general critical incident scene. A crime is often solved within the first few minutes of an investigation, but for the investigator called to a scene identified as a major crime, finding evidence, which has often been destroyed, misplaced, moved, or altered, is a challenge. The scene is always open to anyone in the area within the first moments of the event. By necessity, emergency medical personnel will care for victims without regard to evidence preservation and members of the fire department assure the scene is safe without worrying about evidence destruction, yet First Responders, including the first group of police officers, hold the best recollection of the area in its purest form. Getting to those individuals requires first being aware the individual or emergency crew was on scene. In the chaos that usually follows a critical event, keeping track of those moving in and out the crime scene and in the immediately surrounding areas is impossible.

The first responders to an incident often will not be those who conduct the investigation. Many of the first people on the scene, those responsible for securing the site until relieved, will leave it soon after investigators arrive.

The perimeter of a crime scene, especially in the first minutes after the event, is porous. It offers little containment for investigators and other officials who often arrive to chaos. As depicted in Figure D-1, the goal of perimeter control is the outside solid box, but the reality of it is depicted by the red dashed line. The first task of officials on scene is to mark the outer most boundaries of the event. In an attempt to isolate and identify the area in which most of the evidence may be found, officers will usually use simple yellow ribbon tape to identify the bounds of the crime: **Do Not Cross Crime Scene Do Not Cross Crime Scene Do Not Cross Crime**. Perimeter stabilization is a goal of every investigation whether the scene is a major or minor crime, but regardless of what they do at the onset, the level of scene containment is still represented by the red dashed lines.

Inside the yellow border, police officers, agents, and investigators will try to make sense out of the event that killed, maimed, or otherwise injured human beings and may have caused severe property damage. They will gather evidence, talk to witnesses, and discuss the case details with colleagues. All of those involved with the case will be required to present a report about their findings and all evidence will be recorded. Photographs and measurements will be taken. All the while the scene is being processed, officials will attempt to keep the perimeter secure.

Most agencies have a policy and procedures defining how a crime scene is processed. Often this includes a command post located near the crime scene and a monitor who documents all movements in and out of the area. Still, knowing who may have been inside the perimeter from the time the call came out until it is deemed controlled is impossible.

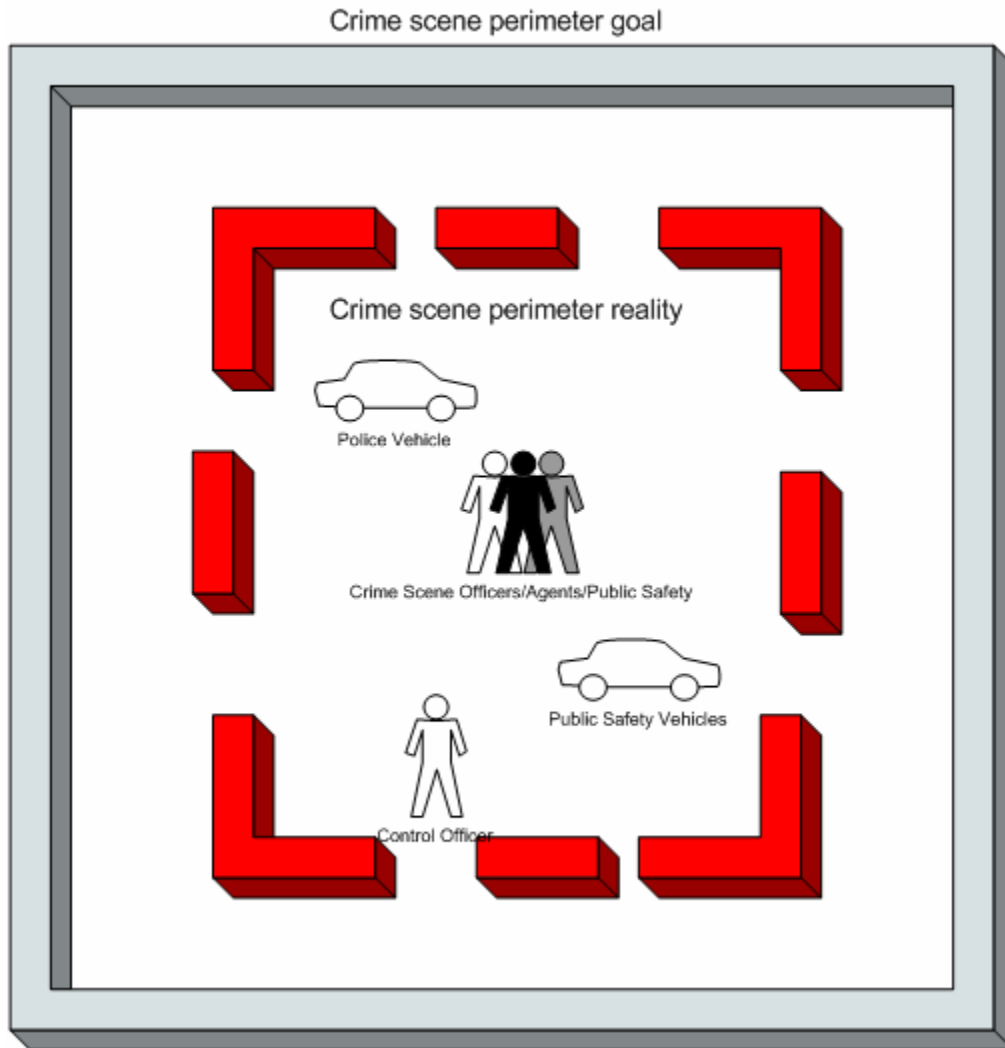


Figure D-1. Crime Scene Perimeter

Maintaining a Record of Officials Near or On a Crime Scene Using RFID

Using a combination of GPS, biometrics identification, and RFID the movements of those carrying a specific device could be tracked and visually displayed on a map. The detail of the map could be enhanced to see the individual's movement across the set boundaries of a crime scene or within the given area. The data set would provide a visual "play back" of movement. Those officers, agents, or public safety personnel who had GPS imbedded in their vehicles could be monitored near the scene and those individuals tagged with an RFID chip could be monitored up to and directly into the scene itself. On playback, the investigator would be able to obtain an accurate date/time of all activities near their scene. It would provide the investigator potential new leads in the case and offer to them a documented list of those officials who were curious onlookers then left and those who stayed and helped with the scene. Either way, those individuals could have bits of evidence otherwise overlooked since the investigator would have no other way of knowing the individuals had crossed into or were near the crime scene.

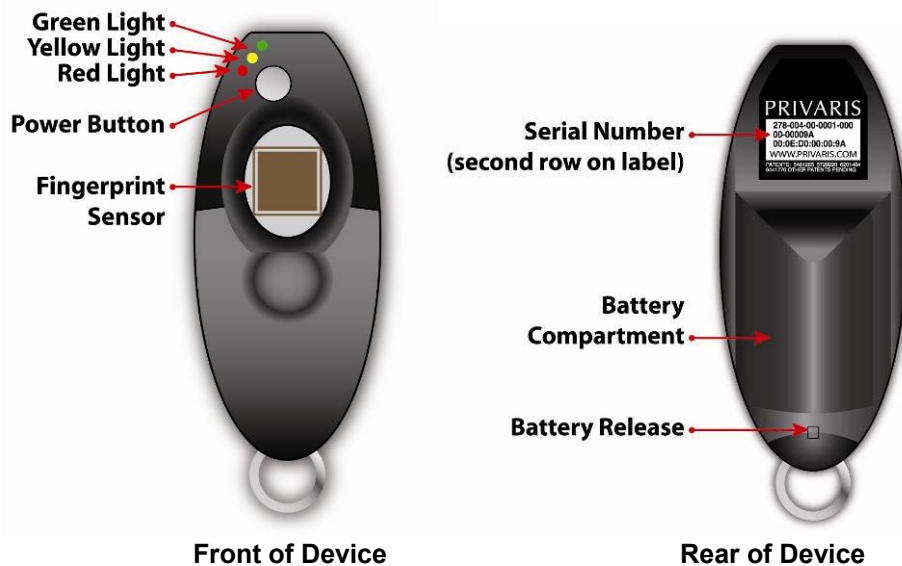
Establishing and Maintaining a Crime Scene Perimeter

The first officer on the scene generally sets up the perimeter. Yellow “Do Not Cross” tape or other physical barriers are used as available. If the officer has access to small location transmitters, the officer would affix these transmitters to or lay on objects around the scene. The perimeter could then be controlled in its totality via a localized GPS. Each official working in the public safety department, the police agency, or the emergency medical agency would be required to carry a location sensor that would communicate to the system.

Another option would be to imbed RFID sensors in the perimeter tape, providing sensing ability around the entire perimeter of the scene. No matter the size of the scene, the area could be monitored in some fashion.

Appendix E Proof of Concept Product Use Information

Simplified Usage Instructions for the Privaris BPID™ LFBT Biometric Device for PHYSICAL ACCESS CONTROL



1. Introduction. The device operates in two modes: low frequency (LF) and Bluetooth. The LF mode is used for badge-like access control applications; the Bluetooth mode is used to transfer stored data files.
2. Power on the device by pressing the power button once to place it in LF mode. (Note that pressing the button twice will place the device in Bluetooth mode.) Yellow light will first glow solid and then begin to flash. The flashing pattern indicates that the device is ready for finger placement.
3. Place an enrolled finger on the sensor. Yellow light will glow solid indicating that the device is acquiring fingerprint images. When a match occurs, the yellow light will go out and the green light will glow. If this does not occur within several seconds, try repositioning the finger slightly one or more times, maintaining the new finger position for two seconds. If a match does not occur after several tries at finger repositioning, you may try to authenticate using an alternative finger that has been enrolled. If a match does not occur within about 20 seconds, the red light will come on. When this occurs, you may cycle power on and off and try again.
4. Once device has been authenticated, touch device to badge reader and door will unlock. The device will automatically power off after approximately 10 seconds.
5. Usage tips.
 - a. Ensure that finger is generally clean and dry prior to placement

- b. Try to place finger on sensor in same position and orientation as during enrollment
 - c. Never press hard or squeeze the device; light pressure generally works best
 - d. Keep finger flat and level with the sensor when placing finger
6. Low battery indicator. A quick red flashing light indicates that the battery should be replaced. Stored information is retained when a battery is replaced.

Note: Privaris, Inc. is the sole vendor of the technology for wireless and biometrics on-device authentication. For more information, see references [30-34].

Acronyms

2D	Two Dimensional
AACPP	Airport Access Control Pilot Program
API	Application Programmer Interface
BAC	Biometric Authentication Credential
BPID™	Biometric Personal Identification Device
CAC	Common Access Card
CAD	Computer Aided Dispatch
CCJT	Center for Criminal Justice Technology (Mitretek Systems)
CO	Corrections Officer
DoD	Department of Defense
EEO	Entry/Exit Officer
GPS	Geographic Positioning System
HR	House of Representatives
HSPD	Homeland Security Presidential Directive
INCITS	InterNational Committee for Information Technology Standards
ISO	International Standards Organization
LF	Low Frequency
LFBT	Low Frequency Bluetooth
MDC	Mobile Data Computer
MDT	Mobile Data Terminal
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
PC	Personal Computer
PD	Police Department
PIN	Personal Identification Number
PKI	Public Key Infrastructure (data encryption)
RFID	Radio Frequency Identification
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential
USB	Universal Serial Bus

