System Assessment and Validation for Emergency Responders (SAVER)

Portable Identification Card Systems Application Note

December 2011

Homeland Security

Science and Technology

U.S. Department of Homeland Security

SAVER

System Assessment and Validation for Emergency Responders

Prepared by: Eastern Kentucky University Justice and Safety Center

Approved for public release; distribution is unlimited.

The *Portable Identification Card Systems Application Note* was funded under Cooperative Agreement Number EMW-2005-CA-0378 between the Federal Emergency Management Agency, U.S. Department of Homeland Security, and Eastern Kentucky University. Photographs included herein were provided by Eastern Kentucky University under the cooperative agreement cited previously, unless otherwise noted.

The views and opinions of authors expressed herein do not necessarily reflect those of the United States Government.

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government.

The information and statements contained herein shall not be used for the purposes of advertising, nor to imply the endorsement or recommendation of the United States Government.

With respect to documentation contained herein, neither the United States Government nor any of its employees make any warranty, expressed or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose. Further, neither the United States Government nor any of its employees assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed; nor do they represent that its use would not infringe privately owned rights.

FOREWORD

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions. Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercial equipment and systems, and provides those results along with other relevant equipment information to the emergency response community in an operationally useful form. SAVER provides information on equipment that falls within the categories listed in the DHS Authorized Equipment List (AEL). The SAVER Program mission includes:

- Conducting impartial, practitioner-relevant, operationally oriented assessments and validations of emergency responder equipment; and
- Providing information that enables decision-makers and responders to better select, procure, use, and maintain emergency responder equipment.

Information provided by the SAVER Program will be shared nationally with the responder community, providing a life- and cost-saving asset to DHS, as well as to Federal, state, and local responders.

The SAVER Program is supported by a network of Technical Agents who perform assessment and validation activities. Further, SAVER focuses primarily on two main questions for the emergency responder community: "What equipment is available?" and "How does it perform?"

As a SAVER Technical Agent, the Eastern Kentucky University (EKU) Justice and Safety Center (JSC) has been tasked to provide expertise and analysis on key subject areas, including communications and incident management systems with a focus on the needs of responders from small and rural communities. In support of this tasking, the EKU JSC developed this *Portable Identification Card Systems Application Note* to provide emergency responders with information about the capabilities, functionality, and use of portable identification card systems that support personnel management and access control. Portable identification card systems fall under the AEL equipment category 04AP-05-CRED, System, Credentialing, which is defined as a software application and associated hardware and material for creating site/event credential badges and controlling scene access.

Visit the SAVER section of the Responder Knowledge Base (RKB) Web site at https://www.rkb.us/saver for more information on the SAVER Program or to view additional reports on portable identification card systems and other technologies.

POINTS OF CONTACT

SAVER Program
Science and Technology Directorate
U.S. Department of Homeland Security
TES Stop 0215
245 Murray Lane
Washington, DC 20528-0215

E-mail: saver@dhs.gov
Web site: https://www.rkb.us/saver

Justice and Safety Center
Eastern Kentucky University
50 Stratton Building
521 Lancaster Avenue
Richmond, KY 40475

E-mail: saver@eku.edu
Web site: http://www.jsc.eku.edu

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION AND SYSTEM OVERVIEW

In July 2011, the U.S. Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA) released the *National Incident Management System (NIMS) Guideline for the Credentialing of Personnel* (DHS/FEMA, 2011), which states that "[s]tate, local, and tribal authorities should card their personnel after completing certification of their identity and qualifications and typing." Like many other paradigm shifts since the September 11, 2001, terrorist attacks, badging has become a more routine and sophisticated process among emergency response agencies.

Partly based on advancements in technologies, identification cards for responders have become more secure and reliable than in the past, allowing Incident Commanders (ICs) to quickly verify the identity and credentials of responders arriving on-scene. Technologies have also advanced to allow for the use of mobile badging systems that may be quickly deployed to an incident scene or facility to read and print cards as well as manage personnel. Portable identification card systems generally encompass hardware and software solutions that are packaged to support personnel management functions, such as accountability, check-in, badging, resource tracking, and demobilization. Agencies may use these systems as end-to-end solutions for managing personnel or for specific incident or event needs, such as the printing of identification cards. Likewise, vendors typically offer emergency responders the flexibility to customize systems based on their requirements. Common to the systems are certain capabilities and portable attributes that allow for their use in various operational environments.

The purpose of the *Portable Identification Card Systems Application Note* is to provide emergency responders with information about the capabilities, functionality, and system uses that support personnel management and access control. Unless otherwise cited, the authors collected information for this application note through Internet research and data collected during the focus group, market survey, and assessment of commercially available portable identification card systems.

For the sake of brevity, the term *system(s)* is used in this document as an abbreviation for *portable identification card system(s)*. Note that the generic term *identification card* is used in this document in reference to the aforementioned equipment name. *Identification cards* are also frequently referenced as *badges* and *credentials* among response agencies, which is consistent with, but not equivalent to, the badging and credentialing processes as defined in NIMS:

- **Badging –** The assignment of physical incident-specific credentials to establish legitimacy and limit access to various incident sites; and
- **Credentialing –** The authentication and verification of the certification and identity of designated incident managers and emergency responders (DHS, 2008a).

Further, the *Federal Information Processing Standards Publication (FIPS PUB) 201-1* defines the term *credential* as "[e]vidence attesting to one's right to credit or authority" (National Institute of Standards and Technology [NIST], 2006). Although agencies may use portable identification card systems to support badging and credentialing, they may also be used for other

purposes, such as identifying and tracking patients among public health and medical professionals, reading state issued driver licenses, and managing information on persons requiring assistance during or following a disaster. Therefore, the generic term *identification card* is used in this report.

1.1 System Overview

Unlike conventional static systems commonly used by response organizations and state departments of motor vehicles for providing identification cards on a regular basis, the focus of this project is on systems that can be easily transported, set up, and re-packaged to allow for use at incident scenes and temporary facilities, such as shelters. Therefore, system hardware and software are packaged to enable their portability and use in various operational environments by emergency responders. As a portable system, the current and potential applications of these systems often vary by discipline, hazard, and the unique requirements of response agencies for controlling scene access and maintaining personnel accountability.

The following sections provide a brief summary of common system components, which fulfill separate, but complementary functions.

1.1.1 Card Printer

Often referred to as the badging application, this component includes a printer and materials for producing cards. The type of printer and its capabilities vary according to the needs of the purchasing agency. For example, the printer may be capable of printing standard letter-sized paper or driver license-sized cards.

The type of card and data stored on the card, which are related to the capabilities of the printer, may vary based on operational and security requirements. For example, a system used for checking in and managing evacuees at a shelter on a temporary basis may only need to produce plastic cards with text. In contrast, planning and coordination for a high-security special event among multiple response agencies may require the issuance of badges embedded with lithographic, holographic, and other security measures and biometric data for verifying the identity of the card holder. This scenario may also require that data be stored on bar codes, magnetic stripes, or smart chips to help streamline the identification of responders and their authorization to access a controlled scene or site during operations.

Card printers may be capable of printing in color and on both sides of the card. Systems in an operational readiness status may be packaged with blank cards, standard paper, ink cartridges, fasteners (e.g., lanyards and belt clips), and other supplies, as necessary. Print material may include durable card stock, labels, and wrist-band material.

1.1.2 Card Reader

This hardware with the associated software or firmware captures data from existing cards for identification and authorization verification, personnel management, and information sharing purposes. Agencies that expect responders to arrive on-scene with an existing card and do not have a requirement for a unique badge may decide to purchase a system with only the card reading capability. The hardware itself is typically a handheld device that is capable of reading bar codes, at a minimum, with a screen for displaying data to the user. The device may be wired to a laptop for transferring data or connected through a wireless network, which would allow for its use at a distance from the computer. Systems may be scalable to allow for the addition of multiple handheld readers to increase the capacity of the system to read and process cards.

Similar to the capabilities of the printer, the capabilities of the card reader to capture data from different types of cards is dependent on the needs of the response agency. Many readers have the capability to collect data stored on magnetic stripes and one dimensional (1D) or two dimensional (2D) bar codes since state-issued driver licenses and responder-specific badges commonly use these features. More sophisticated readers may provide the capability to retrieve biometric information—what is often referred to as a template—from the card holder. This data template may be used for future identity verification or for comparison with an existing database of templates for authorized responders for quick access to the incident scene or event site.

1.1.3 Camera and Computer

The remaining system hardware and software are organized within the Camera and Computer category for the purpose of this report. The camera is often used for capturing a digital image of the person for embedding onto a new card and for storage in the data management software. The camera may be standalone or integrated into the system laptop.

Since these systems are portable, many systems come with a laptop computer that fits within a ruggedized case. The computer supports the management of personnel data and may store data locally on the laptop and/or be connected via a wireless network to an Internet-based application. The computers often come with a Microsoft® Windows® operating system, which supports common workplace applications. The database software is used to store, retrieve, conduct queries, share information, and to populate standard and customizable reports. Systems may allow users to add and manipulate the fields in the database based on their data management and reporting requirements. Also, the computer may come with access controls to allow users to assign privileges for system use and support a broad range of data export, transfer, and security features.

Furthermore, the installed software may support users in designing cards and provide additional functionality for managing personnel and resources. For example, a system with a graphical user interface and configured for sharing data with other check-in sites or with the command post might provide all users with a common operating picture as it relates to personnel management.

In addition to these components, other characteristics may apply to the system as a whole such as the portability of the system, case enclosures, power supplies, and lighting features. See Figure 1-1 for an illustration of the basic system components and their general interaction.

Figure 1-1. Portable Identification Card System Components

1.2 Security and Scalability

Many agencies may require a system with minimal capabilities that are configured to support a rapid deployment and set up at a check-in point to read and provide cards. The time factor associated with many scenarios may be greater than the need for sophistication and heightened card security. Other agencies may require more technology for security or operational reasons. For example, some manufacturers offer the capability to read and print cards with smart chips and radio frequency identification (RFID) technology.

For identity verification and authentication purposes, advanced systems may be able to capture live biometric information, such as fingerprint, iris, or facial images. This data is typically stored in standardized templates on the computer for encoding onto new cards or for future checks and cross-referencing. Security concerns at a controlled scene, facility, or special event may require the capability to authenticate the identity and permissions of responders and workers upon each entry and exit. Some systems also allow users to conduct criminal background checks on all persons entering a controlled area, such as a military installation.

For application at large-scale events or those events with multiple entry/exit points, advanced systems may provide networking capabilities that allow multiple components and/or systems to be used simultaneously and share information in real-time. This can be achieved through the expansion of the number of card readers or the use of multiple complete systems. With abilities to communicate via wired or wireless channels, advanced systems can even be used in regional or state-wide applications thereby allowing multiple systems to be used over a large geographical area. Even if communications channels are not available, some advanced systems can migrate and synchronize data once communications channels are available.

1.3 Guidelines and Standards

Guidelines and standards relating to portable identification card systems may be grouped by operational support and technical elements.

Homeland Security Presidential Directive (HSPD)-5: Management of Domestic Incidents (The White House, 2003) as well as the *National Response Framework (NRF)* (DHS, 2008b) and *NIMS* (DHS, 2008a) provide policy guidance regarding personnel management functions. Accountability of resources is one of 14 management characteristics of NIMS, including check-in, check-out, and resource tracking. Portable identification card systems may support broader requirements for resource management and interface with comprehensive incident decision support software. DHS has also issued guidance on the process of credentialing, which may impact the type and design of identification cards issued by the system. For example, "DHS strongly encourages state, local, and tribal authorities to use FIPS PUB 201-1 and the PIV-I [Personal Identification Verification-Interoperable] guidance in developing their credentialing systems" (DHS, 2011). FIPS PUB 201-1 and PIV-I provide guidance to stakeholders regarding "physical card characteristics, storage media, and data elements" (NIST, 2006).

In addition to national-level policies and guidance, states may have their own resource typing guidelines and system interoperability requirements, which may impact portable identification card system requirements. Reading different types of cards may be an important factor for agencies to consider in order to support mutual aid operations, such as the Emergency Management Assistance Compact (EMAC). In these scenarios, responders may arrive on-scene from out of state with multiple forms of government-issued identification cards.

There are also specifications for technical elements of the portable identification card system beyond the FIPS PUB 201-1 and PIV-I guidelines, which were developed based on *HSPD 12: Policy for a Common Identification Standard for Federal Employees and Contractors* (The White House, 2004). The following organizations provide additional technical standards relating to portable identification card systems:

- The American Association of Motor Vehicle Administrators (AAMVA) provides standards on the design of driver licenses and identification cards;
- The American National Standards Institute (ANSI) InterNational Committee for Information Technology Standards (INCITS) specifies a common set of data elements necessary to support multiple biometric technologies and to promote interoperability of biometric-based application programs and systems; and
- The International Organization for Standardization (ISO) International Electrotechnical Commission (IEC) provides international standards relating to bar code symbology and contact and contactless electronic identification cards, including smart cards and proximity cards.

See Appendix A for a list of Web sites for these organizations.

1.4 Other Considerations

Prospective buyers should take into account various considerations when purchasing a system. Additionally, manufacturers often design systems to meet the specific needs of agencies even though they may advertise a system as "off-the-shelf." Many of these systems consist of commercial parts that may be replaced separately through the manufacturer or other commercial outlets, while some parts may be developed from raw materials and upgraded by the manufacturer. It is common for many systems to include a commercially available printer, card reader, camera, and computer that are integrated, powered, and packaged altogether in a unique manner. Also, many systems include proprietary data management software, such as a Web-based service, which sets many systems apart from the others.

Systems generally cost between $18,000 and $60,000, but prices can increase with the addition of add-ons, upgrades, and options offered by manufacturers. In some cases, manufacturers require monthly fees for those Web-based systems or features scalable to the number of personnel/credentials that are managed by the system in addition to any activation fees. Further, prospective buyers of portable identification card systems must take into consideration other recurring expenditures, such as costs:

- For stocking and replenishing supplies such as print ribbons, laminate, and cards;
- For additional supplies (e.g., batteries, power supplies, antennas);
- Associated with the replacement of the system's electronic parts;
- For support beyond what is provided with the purchase of the system; and
- For upgrading the database management software (Miller & Whelan, 2010).

The type of printed card may be a significant cost factor for agencies, especially those using smart cards with embedded integrated circuit chips that "provide memory capacity and computational capability" (NIST, 2006). Smart cards cost on average $10-$20 per card, while basic plastic cards generally cost from $0.10-$0.25 per card. The costs for the smart cards does not account for initial costs and ongoing fees associated with managing data on the Federal identity and privilege list (IPL) if the goal of the agency is compatibility with FIPS PUB 201-1 and PIV-I requirements.

Most systems may be customized by the end user, allowing them to swap out less desirable capabilities for more desirable ones. There also exists a lack of consensus at the national level for various personnel management practices, which may affect an agency's preferences for one system over another. There are three examples that surfaced during an assessment of systems in June 2011.

First, agencies may prefer that a responder's credentials be maintained on a system computer rather than on the identification card itself. This allows for centralized data management and identification cards that remain active and current even when a responder's credentials change. Conversely, this approach requires that the system reading the card be connected to the responder's host system via the Internet or have access to their database. Some agencies may prefer that identification cards contain a responder's credentials so they may be later extracted from the card and viewed at another site. This model requires that responders carry cards with a complete record of their credentials, which may be important for agencies involved in mutual aid or needing to operate with disparate systems. Potential limitations associated with this model is the need to reprint cards or reprogram smart cards each time a responder's credentials change. See Table 1-1 for a summary of the pros and cons associated with use of 1D and 2D bar codes along with magnetic stripes and smart cards/chips.

Table 1-1. Card Types

Card Type	Pros	Cons
Magnetic Stripe 	✓ Established technology and widely used ✓ Relatively inexpensive	– Lack security features – May become unreadable due to dirt, scratches, and contact with magnetic objects – Limited data storage capacity
1D Bar Code 	✓ Provides centralized data management and security ✓ Only one card needed for each responder regardless of changes to credentials	– Limited to approximately 30 characters of data per bar code – Requires access to host system database for identify and credential verification
2D Bar Code 	✓ May store up to 2,000 characters of data per bar code ✓ Responder credentials accompany responder and may be accessed by disparate systems	– Lack of national consensus on 2D bar code symbology, which may differ from state to state and agency to agency – New card needed when responder credentials change
Smart Cards/Chips 	✓ Provides for security authentication ✓ Data storage available for multiple card purposes ✓ May be reprogrammed	– Relatively expensive cards – Requires infrastructure – Outside of the Federal government, not widely used among response agencies

In addition to decisions regarding types of cards, agencies may differ in their needs for personnel management functionality (e.g., check-in, tracking, demobilization) and how the system is configured to provide this functionality. The June 2011 assessment results reflect how two systems may be configured differently. For example, while the primary computer for one system provided a significant amount of functionality, the handheld device on the other system performed favorably on the criteria relating to personnel assignments and functionality. The operating needs of the agency may determine how best to configure the system to provide these capabilities. For example, agencies may have very specific needs for documentation and reporting on check-in, check-out, etc., in order to facilitate cost reimbursements internally and with outside agencies, including FEMA and other EMAC states.

Requirements for networking are a third factor that may need to be considered when selecting a system. Information sharing between the portable identification card system and other incident decision support software in a community is often required. However, requirements for real-time reporting during an incident may require that systems possess redundant means of sharing information through both wired and wireless networks, including access to the Internet for sharing personnel data with command posts, emergency operations centers (EOCs), and other stakeholders.

2. FUNCTIONS AND APPLICATIONS

There are a variety of potential applications of portable identification card systems that support one or more of the personnel management functions identified in NIMS (DHS, 2008a). For example, systems may be used for supporting the badging process only, which is "the assignment of physical incident-specific credentials to establish legitimacy and limit access to various incident sites" (DHS, 2008a). They may also be used as end-to-end solutions at an incident scene or special event for supporting the:

- Check-in and assignment of responders, volunteers, and other personnel;
- Tracking of personnel, including their locations and welfare, for greater accountability and situational awareness;
- Sharing of personnel information between incident facilities, such as staging areas and command posts or with off-scene EOCs and multiagency coordination (MAC) groups;
- Demobilization of personnel; and
- Documentation of personnel information for cost-reimbursement and other purposes.

In addition to functional requirements, the assessment of the operational environment and associated factors may help agencies determine their need for a portable identification card system versus a static system. The 10 factors provided in Table 2-1 were identified based on feedback provided by a focus group of emergency responders, correspondence with manufacturers, and a review of related literature.

Table 2-1. Operational Considerations

Factors Supporting Use of a Portable System
1. Incident spans multiple operational periods vs. Incident short in duration (less than one period)
2. Incident requires multiagency response vs. Incident requires only single agency response
3. Incident requires large number of responders vs. Incident requires few responders and may be managed using manual processes (e.g., paper)
4. Incident requires access control vs. Incident requires no access control
5. Incident requires temporary badge vs. System for producing long-term identification cards
6. Portable system with easy setup and breakdown vs. Static system for long-term use
7. Packaged for easy vehicular transport vs. Not packaged for vehicular transport
8. Self-powered capability vs. Reliant on external power
9. Backup system to primary with self-contained power supply vs. Primary static system
10. Operational regardless of Internet connection vs. A Web-based application

For incidents spanning a wide geographical area, such as a wildland fire incident, agencies may require the use of a system at a single check-in location or staging area, or deploy multiple systems to manage multiple check-in locations. For dispersed operations that require the use of multiple systems, it may be important for agencies to consider a system's wired or wireless data transfer capabilities provided through an Internet connection or local area network. For

situations that require the reading of existing identification cards for many personnel at one time at a single facility or event venue, agencies may wish to consider purchasing a single system with multiple handheld card readers that can be used in a wireless capacity.

Note that this report does not aim to describe or address operator proficiencies and the required knowledge, skills, and abilities needed to effectively configure and use these products during an incident or special event. The focus of this report should not be interpreted as undermining the importance of other implementation factors such as individual proficiencies and training.

2.1 Common Users, Positions, and Managed Personnel

Common users of portable identification card systems include the traditional public safety disciplines at the local and state levels of government (e.g., fire services, law enforcement, emergency management, public health) as well as private industry. Any type of agency supporting the personnel management function at an incident scene or special event may also benefit from the use of these systems. In addition to agencies at the local and state levels of governments, Federal agencies with units that commonly deploy to an incident scene or manage facilities in support of incidents and special events currently use and may benefit from use of these portable systems. Examples include the U.S. Department of Defense (DOD), U.S. Department of Health and Human Services (HHS), and DHS.

Within the Incident Command System (ICS) structure, the aforementioned functions may be fulfilled by various positions that might likewise benefit from use of the portable identification card system. While the overall responsibility would be that of the IC, the Planning Section Chief or an equivalent organizational element within an agency presumably acts as the Accountability Officer for the incident as well as maintains all documentation associated with the incident. The Planning Section Chief is responsible for the oversight of all "incident-related data gathering and analysis regarding incident operations and assigned resources" (DHS, 2008a).

For expanded and large-scale incidents, the following units and positions may benefit from use

- The **Resources Unit** would likely be responsible for ensuring that personnel check in and the overall tracking and accountability of resources. Many systems provide the capability to complete and manage standard forms and reports such as the Incident Check-In List (ICS 211) and Assignment List (ICS 204).
- The **Demobilization Unit** may use the system to complete the Demobilization Check-Out (ICS 221) form for ensuring the proper release of personnel.
- The **Documentation Unit** may retain system data and reports for cost reimbursement, insurance claims, and historical purposes.
- The **Facilities Unit** under the Logistics Section, which is commonly responsible for managing personnel at shelters and controlling access to facilities, may require a system to badge personnel and check identification and authorization upon each entry and exit.
- Similarly, the **Medical Unit** and **medical specialists** may use portable identification card systems to help identify and track patients and the deceased, as well as to help manage medical facilities and personnel used for providing care and storing and distributing vaccinations, prophylaxis, and other controlled substances.

Similar positions or responsibilities may exist within an EOC or a MAC system that utilizes ICS or configured based on an Emergency Support Function (ESF) structure as described in the *NRF* (DHS, 2008b). At these levels, the emergency responder(s) may be responsible for the following functions that may require the specific or special use of a portable identification card system:

- **ESF #6** – Mass Care, Emergency Assistance, Housing, and Human Services;
- **ESF #7** – Logistics Management and Resource Support;
- **ESF #8** – Public Health and Medical Services; and
- **ESF #13** – Public Safety and Security.

Finally, systems may be used to manage different types of personnel, including responders who may require a unique incident card. Personnel from volunteer organizations, such as the American Red Cross and local community groups, may require special badges to allow for their swift access to shelters and medical facilities. Systems may also be used to identify and manage evacuees under the responsibility of governmental units and nonprofit organizations, persons requiring medical care, and persons with special needs. For managing special events and access to controlled areas, systems may be used to scan pre-made cards for authorized personnel and conduct background checks on other personnel for security purposes.

2.2 Sample Application – Plastics Plant Incident

The following scenario at the local level involving an incident at a plastics plant illustrates an application of the portable identification card system among responders from multiple agencies.

2.2.1 Situation

On a Tuesday morning at approximately 1000 hours, there is a process piping explosion at a plastics plant at 27th Street and Oliver Avenue. Four people are killed outright. Of the remaining 30 person work force, five are seriously injured, five are burned, and three are trapped. Two 5,000 gallon tanks of vinyl chloride are burning with a third exposed. One third of the building's roof has collapsed.

The Central City 911 communications center immediately dispatches a full box assignment to the plastics plant, including Truck 8; Engines 6, 7, and 8; and hazardous material resources from Company 1, Battalion 2, as well as Medic 21 and Ambulance 22. Police Patrol Cars 5 and 7 have also been dispatched.

2.2.2 Initial Response

Upon their arrival on-scene, the deputy fire chief and police chief form a unified command and collectively identify public and responder safety as the initial response objective. The police department is immediately tasked with evacuations and establishing a perimeter with access control at a distance of two blocks in all directions from the plastics plant. The fire chief requests the city's mobile command vehicle and access control equipment, among other equipment.

The commanders form two operational branches for initial response purposes, including Fire/EMS/Rescue and Law Enforcement. They plan to form two additional branches, Health and Public Works, as soon as response personnel assigned to those functions arrive on-scene.

Requirements for access control lead to the identification of specific ingress and egress routes for emergency vehicles following the green arrows identified in Figure 2-1. This figure also displays the entry and exit points near the vicinity of the incident command post and staging area as identified by their respective map symbols.

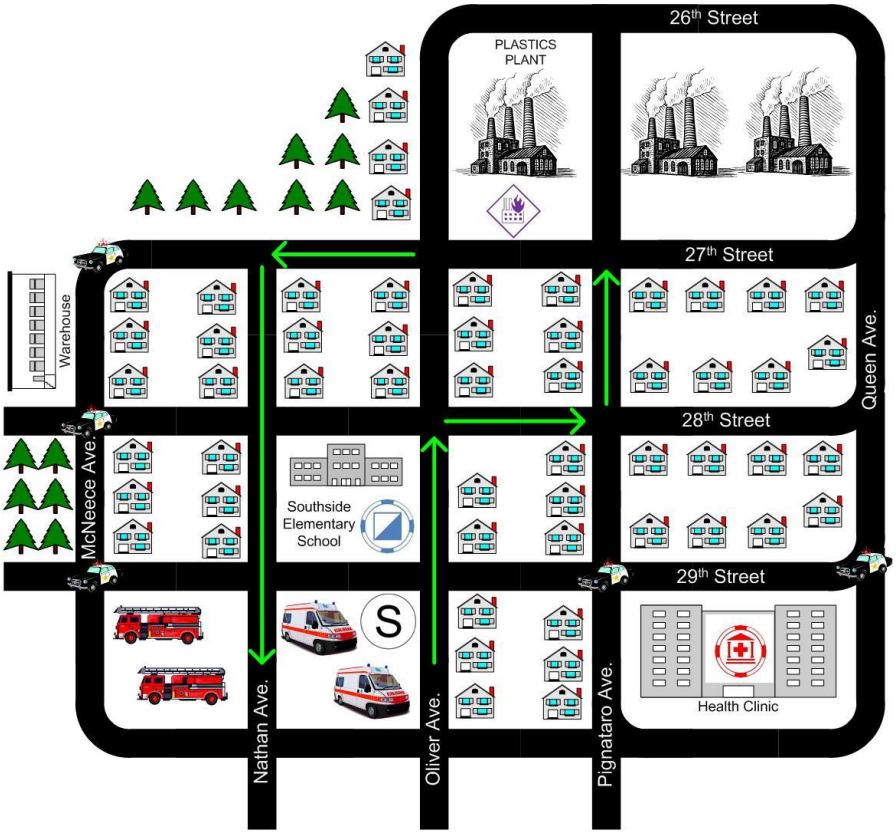


Figure 2-1. Plastics Plant Incident Map Sketch

2.2.3 System Deployment

In support of the operational requirement for access control, staging area personnel deployed one portable identification card system in the vicinity of the staging area with personnel possessing handheld card readers at both entry and exit points of the incident scene. The readers were preloaded with a list of authorized responders from local agencies. For this incident, the users of the system set up the readers to account for responders by branch name, including Fire/EMS/Rescue, Law Enforcement, Health, and Public Works. A second system was set up at the casualty collection point located at the health clinic to support the triage and victim identification process.

2.3 Additional Scenarios

The following scenarios are provided to assist agencies with assessing the need for a portable identification card system. These scenarios are based on real-world situations and information collected through stakeholder interviews and secondary content analysis. Note that these scenarios only represent a sample of many different applications.

2.3.1 Evacuation and Shelter Management

Temporary shelters for emergency purposes may need to be activated for short or extended periods of time and require the identification and management of people who may be carrying a state issued driver license or no identification at all. Personnel staffing and volunteering at shelters may benefit from a portable identification card system to identify persons having special needs (e.g., require medical care and/or planning for short-term housing) or to simply manage in-take and facility capacity. The following case study illustrates this type of scenario.

FEMA/Andrea Booher

Due to its popularity as a retirement state, it is no surprise that Florida's population includes a relatively high percentage of persons who may be classified under the special needs population category, which generally includes the elderly, disabled, and persons requiring medical care (Monroe County Social Services, n.d.). Monroe County, Florida, is the southernmost county in the United States and is made up of parts of the Florida mainland and the Florida Keys, which consist of a 220-mile string of islands connected by U.S. Highway 1 (Monroe County, n.d.). Based on U.S. Census Bureau data from 2009, approximately 17 percent of the county's permanent population of 73,090 is 65 years of age or older, which is nearly four percent higher than the national average for this demographic group (U.S. Census Bureau, 2011).

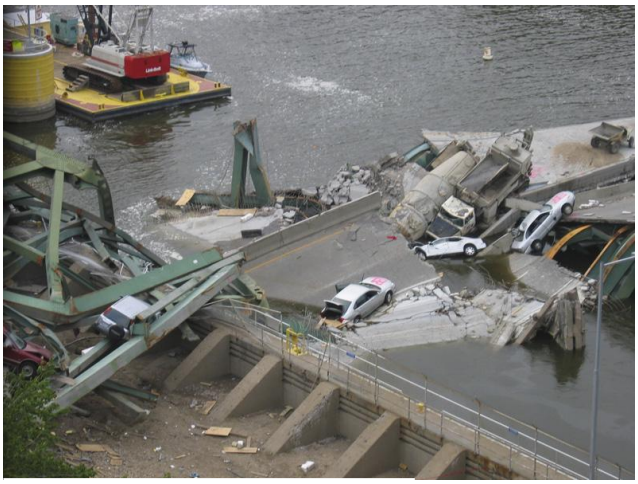
Per the *Monroe County Comprehensive Emergency Management Plan*, special needs individuals are evacuated from the Florida Keys 36 hours prior to a hurricane making landfall (Monroe County, 2007). The evacuation of special needs individuals follows a phased evacuation protocol, which begins with tourists, followed by special needs individuals, and lastly the general public. When evacuations are ordered, special needs individuals in Monroe County are transported by school and charter buses to their designated out-of-county shelter located at Florida International University (FIU) in Miami, Florida. In addition to special needs registry individuals, Monroe County has agreements in place to ensure hospital patients within the Florida Keys are safely evacuated as well.

When an evacuation is ordered, Monroe County activates its mutual aid agreement with FIU, which provides use of the FIU's Recreation Center as a shelter for the evacuated special needs individuals that includes special provisions. Within the recreation center, those individuals who require medical attention are placed in a specific area separate from the general evacuees. The shelter is administered by the Monroe County Health Department and the American Red Cross, which has agreements with local restaurants to provide food services to the evacuees. Monroe County activates additional agreements with nursing homes within Broward County, Florida, for placement of those special needs individuals who are considered medically fragile and require attention beyond what can be provided in the FIU special needs shelter.

The diversity of stakeholders operating at the shelter and requirement that staff provide constant medical care and general assistance to evacuees may benefit from a portable identification card system that can be easily set up and operated.

2.3.2 Patient Management

Portable identification card systems may be used for maintaining accountability of injured persons as to their type of injury and transported location, among other critical information. Not only do systems allow medical personnel to track patients, but they may print triage information on materials such as wristbands and tags. The use of triage tags with bar codes may support the quick identification of victims, their triage status and initial diagnosis, and associated belongings. The following case study illustrates a type of scenario that may benefit from use of a portable identification card system.



FEMA/Todd Swain

On August 1, 2007, during evening rush hour, the central span of the Mississippi River Bridge in Minneapolis, Minnesota, crumpled. The entire structure collapsed into the river and riverbanks. Officials estimate as many as 100 vehicles and their occupants plunged into the river, the riverbank, and a local rail yard (U.S. Fire Administration [USFA], 2007). Thirteen people were killed and 121 were injured as a result of the collapse (USFA, 2007). Local emergency personnel, as well as those from neighboring cities and counties, took part in the rescue and recovery efforts.

According to a lessons learned report (USFA, 2007), there were significant issues in the management and tracking of patients during the incident response. In fact, the emergency medical control center responsible for tracking victims and notifying local hospitals only accounted for 20 percent of all patients during the incident because of a lack of communications and failure of medical personnel to follow plans and procedures, among other reasons. As a result, hospitals received only vague information regarding the victims. Also, the patient identification tags were not used consistently during the incident, which "compromised the identification of patients and hospital destinations" (USFA, 2007).

Although these findings suggest many areas for improvement, the sharing of victim information between personnel on-scene and facilities and the tracking of victims may be supported through use of a portable identification card system potentially in conjunction with other information management systems that provide standard formats for exchanging information.

For example, the Emergency Data Exchange Language Hospital Availability Exchange (EDXL–HAVE) standard allows for the seamless communication of the status of a hospital, its services, and resources, such as bed capacity and availability, emergency room status, services provided, and available medical staff. Portable identification card systems installed with applications compatible with the EDXL-HAVE standard would allow medical personnel to not only identify victims and their initial diagnosis, but also determine where to route victims with minor injuries as opposed to those with critical life-threatening injuries.

2.3.3 Planned Event

In some communities, annual events or major sporting events not only bring in attendees that sometimes double the local population, but they may require additional staff from outside entities for increasing security and emergency medical services, among other needs. They often require the management of event staff and volunteers. This scenario involves the use of the system to account for and provide easy identification for the different categories of personnel involved in the planning, coordination, and execution of a planned event.

FEMA/Jocelyn Augustino

During the 45th Democratic National Convention (DNC) held from August 25-28, 2008, approximately 35,000 people converged on Denver (Denver Office of Emergency Management and Homeland Security [DOEMHS], 2009). Most of the events for the DNC were held in or around the Pepsi Center in downtown Denver and Invesco Field at Mile High. Other events related to the DNC were held in various locations across the city (DOEMHS, 2009).

Due to the planning efforts of the city, county, and surrounding communities, the DNC concluded with no major incidents, no property damage, and roughly 154 DNC-related arrests (DOEMHS, 2009). However, the after action report issued by the city and county of Denver following the event indicated that "[t]he number and type of different credentials led to some confusion and much redundancy" (DOEMHS, 2009). There were at least five different government agencies issuing credentials for different aspects of the event and select event workers were required to obtain multiple credentials to do their jobs. This led to the recommendation that "[t]he number and type of different credentials should be reduced and kept as simple as possible" (DOEMHS, 2009).

Portable identification card systems may be used to produce unique event badges to help overcome multiagency coordination challenges similar to the ones experienced in Denver in 2008. They may be used on a large scale among all stakeholders, or for issuing cards and managing the entry of select participants such as volunteers and event workers at separate venues. In the case of the Denver experience, for example, the after action report indicated that food inspectors required five different credentials in order to access event venues (DOEMHS, 2009).

3. CONCLUSION

In summary, this application note provides information about the capabilities, functionality, and use of portable identification card systems, which may assist emergency responders in the management of personnel at an incident scene, special event, and/or supporting facility. The systems may be used as end-to-end solutions for managing personnel or for a specific incident or event need, such as badging and/or personnel tracking. Although systems come with many of the same features found in static identification card systems, such as card printers and readers, their portable attributes allow for their use in various operational environments.

Please note that equipment with software tends to evolve very quickly as compared to the hardware components; new versions of software with new capabilities are generally released more often than their hardware counterparts. Emergency responders need to manage these changes and account for the other considerations identified in Section 1.4 when purchasing and using portable identification card systems.

APPENDIX A – REFERENCES

American Association of Motor Vehicle Administrators (AAMVA): http://www.aamva.org/.

American National Standards Institute (ANSI) InterNational Committee for Information Technology Standards (INCITS): http://www.ansi.org.

Denver Office of Emergency Management and Homeland Security. (2008). *City and County of Denver 2008 Democratic National Convention After Action Report*. Denver, CO: Denver Office of Emergency Management and Homeland Security.

International Organization for Standardization (ISO) International Electrotechnical Commission (IEC): http://www.iso.org/.

Miller, R., & Whelan, M. (2010). *Resource Accountability Guide for First Responders*. Traverse City, MI: Salamander Technologies, Inc.

Monroe County. (n.d.). About Monroe County. Retrieved from: http://www.monroecounty-fl.gov/index.aspx?NID=27.

Monroe County, Florida. (2007). *Monroe County, Florida Comprehensive Emergency Management Plan*. Key West, FL: Monroe County, FL.

Monroe County Social Services. (n.d.). Special Needs Registry. Retrieved from: http://www.monroecounty-fl.gov/index.aspx?NID=148.

National Institute of Standards and Technology (NIST). (2006, March). *Federal Information Processing Standards Publication (FIPS PUB) 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors*. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from: http://csrc.nist.gov/ publications/fips/ fips201-1/FIPS-201-1-chng1.pdf.

Responder Knowledge Base (RKB): https://www.rkb.us.

The White House. (2003, February 28). *Homeland Security Presidential Directive 5: Management of Domestic Incidents*. Retrieved from: http://www.dhs.gov/xabout/laws/gc_1214592333605.shtm.

The White House. (2004, August 27). *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors*. Retrieved from: http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#1.

U.S. Census Bureau. (2011, June 3). State & County QuickFacts – Monroe County, Florida. Retrieved from: http://quickfacts.census.gov/qfd/states/12/12087.html.

U.S. Department of Homeland Security (DHS). (2008a, December). *National Incident Management System*. Washington, DC: U.S. Department of Homeland Security. Retrieved from: http://www.fema.gov/emergency/nims/.

U.S. Department of Homeland Security (DHS). (2008b, January). *National Response Framework*. Washington, DC: U.S. Department of Homeland Security. Retrieved from: http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.

U.S. Department of Homeland Security/Federal Emergency Management Agency (DHS/FEMA). (2011, July). *NIMS Guideline for the Credentialing of Personnel*. Washington, DC: U.S. Department of Homeland Security. Retrieved from: http://www.fema.gov/pdf/emergency/nims/nims_alert_cred_ guideline.pdf.

U.S. Fire Administration (USFA). (2007, August). *Technical Report Series: I-35W Bridge Collapse and Response (USFA-TR-166)*. Retrieved from: http://www.usfa.fema.gov/downloads/pdf/publications/tr_166.pdf.

APPENDIX B – ACRONYMS/ABBREVIATIONS

The following acronyms/abbreviations are commonly used in this document.

Acronym/ Abbreviation	Definition
1D	One Dimensional
2D	Two Dimensional
AEL	Authorized Equipment List
DHS	U.S. Department of Homeland Security
DNC	Democratic National Convention
DOEMHS	Denver Office of Emergency Management and Homeland Security
EDXL-HAVE	Emergency Data Exchange Language Hospital Availability Exchange
EKU	Eastern Kentucky University
EMAC	Emergency Management Assistance Compact
EOC	Emergency Operations Center
ESF	Emergency Support Function
FEMA	Federal Emergency Management Agency
FIPS PUB	Federal Information Processing Standards Publication
FIU	Florida International University
HSPD	Homeland Security Presidential Directive
ICS	Incident Command System
JSC	Justice and Safety Center
MAC	Multiagency Coordination
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NRF	National Response Framework
PIV-I	Personal Identify Verification-Interoperable
RKB	Responder Knowledge Base
SAVER	System Assessment and Validation for Emergency Responders
S&T	Science and Technology Directorate