FEMA

NIMS Standards Case Study: Responder Authentication

National Preparedness Directorate

August 2008

Utilizing Biometrics to Identify Responders in the National Capital Region

In the immediate aftermath of a disaster, an emergency responder reports to the incident scene, offering his/her expertise to response agencies. While the responders on-scene can use the support as they work to save lives and protect property, incident commanders know they must manage access to the incident scene and have no instantaneous way to verify the identity of individuals offering support. Managing responders from outside jurisdictions can pose a significant challenge for incident commanders. Identity verification at an incident perimeter is dependent upon responders recognizing an identification card and believing it to be credible. Each jurisdiction maintains its own badges for its responders. These badges typically are not formatted in a similar manner and do not carry the same information. Access for responding agencies may be dependent upon the responder at the incident perimeter being personally familiar with the badges of a non-local jurisdiction. Similarly, identification cards that rely solely on photo identification for identity verification may be more likely to be misused by unauthorized personnel wishing to gain access to an incident scene.

Advancements in biometric technology and the development of biometric tools for the public safety realm have begun to provide solutions to identity verification issues. Such technologies, when integrated into emergency management plans and processes, can be a powerful tool for emergency response organizations in both meeting day-to-day operational needs and disaster response. This article highlights pilot programs that are using biometric technology to support identity verification systems. Further, it illustrates how biometric standards, such as the **American National Standards Institute (ANSI) International Committee for Information Technology (INCITS) 398: Information Technology – Common Biometric Exchange Formats Framework (CBEFF)**, support the concepts of the National Incident Management System (NIMS).

ABOUT THIS CASE STUDY

While NIMS provides a common structure and terminology for responding to incidents and planned events, voluntary consensus standards support NIMS implementation by creating uniformity of use and practice. Such support is particularly important for prepardness and incident management. Standards also provide:

- Accepted and uniform criteria for measuring the adequacy of preparedness efforts and performance of emergency operations;
- Technical guidance; and
- Common resource descriptions to facilitate mutual aid—the sharing of resources among jurisdictions.

The National Preparedness Directorate (NPD), Federal Emergency Management Agency (FEMA) and the NIMS Support Center (NIMS SC) work in partnership with standards development organizations (SDOs) to identify existing industry standards that support NIMS implementation. These select standards are placed on the NIMS Recommended Standards List (RSL) and posted on the FEMA website for public information.

Recognizing the potential value of biometric technology to responders, the NIMS RSL includes the ANSI INCITS 398: Information Technology – CBEFF standard. The ANSI INCITS 398 standard was developed out of a joint effort between the National Institute of Standards and Technology (NIST) and the Biometric Consortium to identify a “technology-blind” biometric format that would provide a common structure for exchanging biometric data without prescribing particular technological solutions.[1] The first such standard was published as NISTIR 6529 and, in 2005, a revised version of this standard was published as ANSI INCITS 398-2005.

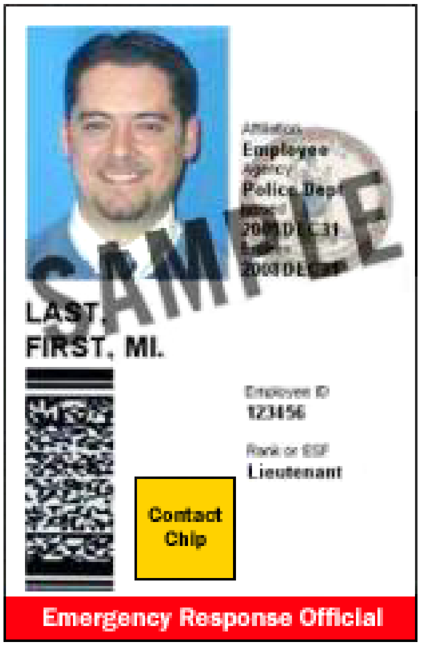
As reflected in ANSI INCITS 398-2005, the CBEFF describes a set of data elements necessary to support biometric technologies in a common way. These data elements can be placed in a single file used to exchange biometric information between different system components or between systems themselves. The result promotes interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange Specifically, ANSI INCITS 398-2005 supports multiple biometric data types (e.g., fingerprint, face and voice recognition, etc.) and/or multiple biometric data blocks of the same biometric type. It also defines biometric data objects for use within smart cards and other tokens and describes common fields for biometric features and the validity period.

An updated version of the ANSI INCITS 398 standard was approved and published in 2008. The 2008 edition adds two new formats: Biometric Information Data Objects for Use within Smart Cards or Other Tokens and CBEFF Patron Format B, a simple root header for use in domains where one or more patron format may be encountered. Additional information has also been provided on CBEFF patrons, the current list of patrons, and how to apply for a new CBEFF patron. A CBEFF patron is defined as “[a]n organization that has defined a standard or specification incorporating biometric data objects that conform to CBEFF.” Revised definitions and reorganization of other materials have clarified concepts and terminology and made the 2008 edition easier to use.

The CBEFF structure defined in ANSI INCITS 398 has been incorporated into other standards and guidelines which involve the interchange of biometric information such as fingerprints. Of particular relevance to the emergency response community, the CBEFF is integrated into Federal Information Processing Standard (FIPS) 201, the standard for Federal government identification cards to ensure compliance with Homeland Security Presidential Directive 12 (HSPD – 12), which states that wide variations in the quality and security in forms of identification used to gain access to secure facilities need to be eliminated. HSPD-12 outlines a policy to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal government to its employees and contractors. Under FIPS, any biometric data in an agency’s Personal Identity Verification (PIV) model (e.g., fingerprints) must be embedded in the CBEFF structure, which means that all Federal identification cards conforming to HSPD-12 and FIPS use the CBEFF structure for embedding fingerprints. The following section features an application of CBEFF through FIPS: a responder identification smart card piloted in the City of Alexandria, Virginia.

OVERVIEW OF ALEXANDRIA FRAC PROJECT

The September 11th attack on the Pentagon brought about a massive mutual aid response effort from jurisdictions throughout the National Capital Region (NCR). In an uncertain security environment and while needing to regulate access to sensitive areas of the Pentagon, Arlington County (Virginia) responders, responsible for incident command, struggled to rapidly verify the identity, qualifications, and authorizations of arriving officials from Federal, State, and local agencies. Captain Eddie Reyes of the Alexandria Police Department, arriving at the Pentagon on September 12th to support Arlington’s response efforts, described a scene of “confusion and chaos at the perimeter” and, like other legitimate responders, was initially denied site access. Subsequent incidents in the NCR, including the 2001 anthrax attacks, the 2002 sniper incident, and a May 2005 violation of the NCR no-fly zone, highlighted the need for a common means of identification for response agencies operating in the NCR.



Cooperation between the Department of Homeland Security (DHS) Office of National Capital Region Coordination, the State of Maryland, the Commonwealth of Virginia, the District of Columbia, and other jurisdictions within the NCR resulted in the First Responder Partnership Initiative (FRPI). Working in consultation with product vendors, this effort produced a common “smart” identification card, known as the First Responder Authentication Credential (FRAC) card, embedded with biometric information which could be validated through common processes by response agencies throughout the region. The City of Alexandria participated in the pilot FRPI program and was an early implementer of a smart card identification program for its emergency responders.

Alexandria is located in close proximity to the Pentagon and responders from the city provided mutual aid support to Arlington County responders operating at the Pentagon on September 11th. Alexandria is also home to a number of Department of Defense (DoD) facilities and its responders work closely with the Pentagon Force Protection Agency (PFPA) and other DoD agencies. Due to its strategic location within the NCR and its frequent interaction with Federal, State, and local response agencies, Alexandria was one of two jurisdictions chosen by the Virginia Department of Transportation (VDOT) as a pilot site for implementing the FRAC identification card program. Mark Penn, Emergency Management Coordinator for Alexandria, stated that the city participated in the FRAC program to meet two goals: first, to develop a common responder credential for use throughout the region; and secondly, to secure critical infrastructure by leveraging existing technology to strengthen access controls.

The VDOT had lead responsibility for defining the requirements for the FRAC card distributed in Alexandria and Arlington. In doing so, VDOT looked to FIPS 201, the standard for Federal government identification cards to ensure compliance with HSPD-12. While FIPS 201 is not a requirement for State or local governments, VDOT and others have used this standard to guide their own smart card programs. Using the FIPS 201 standard as guidance, VDOT worked with Alexandria and Arlington to create the FRAC, a high-tech identification card designed to:

- Securely establish emergency responders' identities at the scene of an incident.
- Confirm responders' qualifications and expertise, allowing incident commanders to dispatch them quickly and appropriately.
- Enhance cooperation and efficiency between State and local responders and their Federal counterparts.[2]

As part of the pilot program, Alexandria issued over 1,000 FRAC identification cards to police, sheriff's office, firefighter, emergency medical service, and emergency operations center staff. Recipients included both sworn personnel and civilian support staff. Mark Penn served as Alexandria's single point of contact for FRAC management and distribution and solicited lists of personnel authorized to receive a FRAC card from each emergency service department within the city. Individuals identified to receive a FRAC card were required to provide their credentials and a secondary form of photo identification (typically a driver's license), sign a release form, and provide multiple fingerprints via a digital fingerprinting station. The FRAC recipients provided additional information on their attributes, expertise, and certifications. This data can be used for asset management by incident managers to identify the skill sets of responders participating in a multi-agency and/or multi-jurisdictional response. Finally, FRAC recipients provided personal information, such as blood type and medical conditions; this information can be used by other responders should the FRAC card holder be injured during a response effort.

> "In a nutshell, the FRAC card contains all relevant information about a first responder that would be needed in a major incident. If there was a major event (such as another 9-11, a tornado, hurricane, hazmat incident, etc.), a first responder would respond to the scene and present his FRAC card at the incident command. The card would contain information about that first responder that would help the incident commander efficiently deploy resources."
>
> – Sergeant Ben Bolton, Alexandria Police Department

Implementation of a smart card program is not without its issues, however. Some of these issues are technological, such as how well will fingerprint readers work in inclement weather or in a "dirty" field environment. Other issues are programmatic. As Captain Eddie Reyes of the Alexandria Police Department observed, processes must be put in place to periodically vet the FRAC recipients list to ensure that responders who have left their respective departments no longer have active FRAC cards and to ensure that newly hired staff receives FRAC cards. Training programs must also be established so that responders are familiar with the FRAC card capabilities and the information contained therein. Finally, use of the FRAC cards should be periodically tested, both during exercises and in the day-to-day work environment, to confirm that responders are familiar with using the cards. Maintaining such a program involves a substantial financial cost for the implementing jurisdiction. Mark Penn has cited the high cost associated with the FRAC program as a significant reason why Alexandria has not widely implemented the program following the end of the pilot. Regardless, officials from Alexandria hope to continue implementation of the FRAC program based on the benefits identified during the pilot.

CONCLUSION

The FRAC program implemented in Alexandria highlights how biometric technology can be applied to support responders. The NPD has recognized that biometrics may be a valuable tool to responders, and has placed the ANSI INCITS 398: Information Technology – CBEFF standard on the NIMS RSL, indicating that this standard supports implementation of the NIMS requirements. Biometric technology is in a constant state of evolution and, in many instances, costs can inhibit implementation of these technologies at the State and local levels. However, as the scope of biometric technology expands, responders may be able to identify further opportunities to develop and implement powerful biometric tools to allow them to execute their roles more effectively. At the same time, NPD and the NIMS SC continue to monitor standards development activities to identify biometric standards that will assist responders in achieving NIMS implementation.

RESOURCES

National Incident Management System (NIMS) Standards
http://www.fema.gov/emergency/nims/nims_standards.shtm

American National Standards Institute
http://www.ansi.org/

Virginia FRAC
http://www.virginiafrac.com/

Biometric Consortium
http://www.biometrics.org/

REFERENCES

NIMS SC staff obtained information for this case study through interviews with key personnel from the respective case study locations, as well as online research. Unless otherwise cited, all information presented in this study is drawn from these interviews.

[1] NISTIR 6529-A, Common Biometric Exchange Formats Framework (CBEFF), April 5, 2004.

[2] “Alexandria Becomes First City in United States to Implement New System to Authenticate Credentials of First Responders At Emergency Scene,” April 3, 2007.

FRAC Identification card photo courtesy of Government Technology. “Virginia First in Nation to Issue New First Responder Credentials,” March 13, 2007. http://www.govtech.com/gt/articles/104398 Accessed August 8, 2008.

To support NIMS implementation, DHS established the NIMS Support Center in 2005 -- a program that operates under a cooperative agreement between FEMA and the Justice and Safety Center, Eastern Kentucky University. The NIMS Support Center develops new responder tools, enhances technology integration and interoperability, and provides technical assistance and support to the incident management and response community. For additional information about the NIMS Support Center or this publication, please e-mail the staff at: FEMA-NIMS@dhs.gov.