

KNOWING WHO'S WHO

NEW REALITIES ELEVATE THE IMPORTANCE OF IDENTITY MANAGEMENT

SYSTEMS AND SECURE ID CARDS

ORIGINALLY PUBLISHED IN SECURITY PRODUCTS

IN THE UNITED STATES, THE DEPARTMENT OF HOMELAND SECURITY consolidates 22 agencies under an \$18 billion budget. The department employs 180,000 people and unifies once-fragmented federal functions to create a single agency dedicated to protecting America from terrorism. It gives power and resources to federal, state and regional agencies, and charges them with the task of safeguarding the country and its people.

Outside of the United States, national and regional government agencies are creating their own organizations dedicated to preventing terrorism and minimizing its aftermath if an event were to occur. The reaction to Sept. 11, 2001, and the lessons learned stretch far beyond U.S. borders.

When these homeland security professionals — and their counterparts in other countries — respond to a terror-based threat or event, they will almost always be managing a "scene." Effectively protecting victims, bystanders, authorized personnel, emergency vehicles, evidence, communications systems and other critical items that comprise these scenes will require homeland security professionals to quickly secure areas in the face of chaos. When you recall images of Sept. 11, it's obvious that creating a secure and highly controlled environment will almost always be a monumental challenge for security organizations in the United States and around the world, especially in the areas of accountability, verification and scene access.

In addition to biometrics and digitally stored photos, today's identification systems provide security organizations with the ability to visually differentiate their official ID cards or badges.

Fortunately for homeland security professionals, key technologies — such as biometrics, smart cards, image capture, ID card printing and data management — have evolved to the point that remote and rapid deployment of identification systems is extremely easy and highly effective. With these technologies, organizations that counter, investigate and cope with terrorism now have the tools they need to produce and manage the highly secure credentials that help make a scene secure.

ID SYSTEMS ENHANCE ACCOUNTABILITY

AS HOMELAND SECURITY ORGANIZATIONS PREPARE plans for a variety of possible emergencies, they are realizing the importance of accountability on two very distinct levels.

The first is general accountability for people who enter or leave a disaster scene. Many homeland security professionals have discovered that highly secure identification cards — augmented with photos or biometrics stored on smart cards or 2D bar codes — allow them to know who has entered a scene, who is still on a scene and who has left. Remote, handheld devices can scan a chip or bar code on each ID card, authenticate the person's identity and record where that person is working.

For example, if a corporate or government facility is being threatened or has been damaged by an act of terror, security teams can use handheld scanners to read photo ID cards, determine if a person is presenting the credential they were issued in a secure setting and determine if the credential itself is authentic.

The second level of accountability concerns equipment, especially emergency vehicles. Homeland security professionals are keenly aware that if official emergency vehicles are stolen and controlled by the wrong people, they can be used to perpetrate a variety of crimes. For example, if an ambulance or fire engine is unaccounted for and stolen, it could be loaded with explosives, driven into a scene and detonated.

Identification systems with remote capabilities allow site commanders and other key personnel to quickly and accurately identify people who are in control of emergency vehicles. Even if unwanted intruders were able to forge official-looking ID cards with their actual photos and names on them, a quick scan of a smart chip or 2D bar code is likely to betray them.

THE VALUE OF INSTANT VERIFICATION

HANDHELD SCANNING DEVICES AND ID CARDS WITH smart chips or 2D bar codes also provide important verification capabilities for homeland security organizations and similar international groups coping with disaster scenes.

Frequently, disaster teams bring together professionals from a variety of disciplines. The process happens rapidly in chaotic environments and requires coordinators to marshal teams of people who have likely never met before. In these circumstances, it is vital to scene security and the speed of development that coordinators have a fast, easy and reliable way to verify the identity of any individual on any team and ensure that person receives appropriate site access.

Information scanned from ID cards during a disaster can be captured and stored for easy access and report generation. After an event, security personnel can retrieve this information and use it to paint a clear picture of who was there, when they arrived, where they worked and when they left.

In addition to biometrics and digitally stored photos, today's identification systems provide security organizations with the ability to visually differentiate their official ID cards or badges. For example, they can color-code badges to determine who should be in specific places at a scene. Color-coding could indicate if personnel should be working on the perimeter, in an operations center, in a radio command center, in a newsroom or in a shelter.

NEW IDENTIFICATION TECHNOLOGIES

NOT LONG AGO, ID CARDS WERE PRODUCED USING a simple cut-and-paste process. Anyone with an instant camera, a laminator and access to a decent color printer could forge or alter a photo ID card fairly easily. The lines of defense were not very strong. Also, photo ID cards were used almost exclusively for visual identification.

Determining whether an ID card was authentic or if a person was presenting a credential that was issued as part of a secure process was essentially a judgment call. Security guards and others who controlled access to facilities or restricted areas had to trust their instincts and had little, if any, technology on their side.

But ID card technology made a huge leap about 10 years ago when digital photo ID systems were introduced. Instead of cutting and pasting and using film-based images, digital photo ID systems allowed corporations, government agencies and other security-minded organizations to capture images digitally, store them securely and print them directly onto plastic cards. As a result, digitally produced photo ID cards are much harder to forge or alter than previous film-based IDs.

Since the introduction of digital photo ID systems in the mid 1990s, solutions providers have made great advances in technologies that make ID cards secure and resistant to fraud. These breakthroughs include highly secure topcoats and overlays, laser engraving, microtext and optical variable devices.

OVDs are design elements on photo ID cards that can be identified only under specified optical conditions. They cannot be duplicated or recreated using color copiers, scanners or printers. OVDs include holograms and guilloché patterns — similar to those found on many national currencies — that appear when a card is rotated under normal lighting conditions. OVDs also may include microscopic printing that appears under magnification and specialized inks that appear only when exposed to black light or laser light.

Combining multiple OVDs exponentially increases the security of a photo ID card. For example, corporations and government agencies use customized holograms that are nearly impossible to replicate to protect cards from alteration. Any attempt to alter a photo or text on a card disrupts the hologram and makes fraudulent activity easy



to identify. In addition to customized holograms, corporate and government agencies are using text that is either hidden or laser-engraved below the surface of a card. When security guards and other authorized personnel have the equipment and knowledge to look for these elements, alterations and forgery become difficult — even for the most accomplished criminal.

This level of verification, authentication and security is critical for homeland security organizations both in day-to-day operations and in the face of disasters. Knowing that individuals at a disaster scene can be identified through a legitimate ID card issuance process is key to strong, effective organizational security.

THE POWER OF MACHINE-READABLE TECHNOLOGIES

IN ADDITION TO OVDS, TOPCOATS, OVERLAYS AND printing technologies, photo ID cards have become much more secure and powerful because of machine-readable technologies, such as smart cards and 2D bar codes.

In the past, photo ID cards may have included an encoded magnetic stripe or ordinary bar code. This allowed cards to be used for access control systems and other relatively simple tasks that did not require much data to be stored on a card.

Today, however, solutions providers give organizations the option of adding smart card chips or 2D bar codes to their ID cards. The storage capacity of these machine-readable technologies allows organizations to store photos or biometric images — such as fingerprints or handprints — on their ID cards. Then, when someone presents a credential, the card can be scanned or inserted into a reader with an integrated biometric scanner. Authorized personnel can then check to ensure that the person presenting the card, the photo printed on the card and the photo or biometric image stored on the card all match.

This multi-factor identification process is ideal for homeland security teams working at disaster scenes. Even in a chaotic environment, authorized personnel can quickly verify the identities of those entering and leaving a scene, as well as track the movements of authorized personnel for a variety of safety and security reasons.

This article originally appeared in the January 2005 issue of Security Products, pgs. 62-64. It can be found at www.secpdonline.com.



NEW ENGLAND SECURITY & COMMUNICATIONS

9 Main Street • Suite 4B
PO Box 421 • Manchaug, Ma 01526-0421
Tel: +1 800 487-6371 • +1 508 476-9200
Fax: +1 508 476-9333
sales@badgebuilder.com