NLECTC National Law Enforcement and Corrections Technology Center
A program of the National Institute of Justice
TECH b•e•a•t
From Winter 2010 *TechBeat*
Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections and Forensic Sciences

First Responder Credentials Expedite Access

During an emergency involving multiple jurisdictions, having a trusted means to rapidly identify law enforcement and other responders is essential. An evolving federal credentialing program is providing that capability, along with other uses.

The technology used in the credentials, known as First Responder Authentication Credentials (FRACs), provides trusted and electronically validated identification, interoperable across federal, state and local jurisdictions. Identity authentication checks are made easily at an emergency scene, where a handheld reader device or a laptop in a law enforcement cruiser can verify the individual's identity.

The U.S. Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) have been working with state agencies for several years in a series of pilot demonstrations to test various emergency scenarios using the credentials. The goal is to encourage adoption and operational use of high assurance authentication credentials nationwide.

The FRAC effort is part of a broader enterprise strategy to leverage investments, innovations and enhanced capabilities of Personal Identity Verification (PIV) credentials being issued to all federal employees and government contractors. In 2004, Homeland Security Presidential Directive 12 (HSPD 12) mandated new standards for secure and reliable personal identification for federal employees and contractors. The credentials are to be used for accessing federal buildings and computers. The National Institute of Standards and Technology issued the standard for credentialing employee identification credentials (Federal Information Processing Standard (FIPS) 201-1).

FRACs use the same technology as PIV credentials. They contain encrypted identification information, including name, agency and two fingerprints. A credential holder has a personal identification number (PIN) that must be entered into a credential reader to allow access to the credential's information.

"It allows incident commanders to make a better, informed decision about who to allow in," says Thomas Lockwood, senior advisor for the DHS Screening Coordination Office. "You have a very high level of assurance that the person is who he/she claims to be."

The scenario demonstrations using FRACs have included federal, state and local emergency response officials as well as utility companies and transportation agencies. Reaction from emergency response officials who have participated in demonstrations has been positive, says Craig Wilson, Federal and Mutual Aid Emergency Response Official Coordinator for the FEMA Office of National Capital Region Coordination.

"When asked if the technology gave law enforcement officials the ability to make an informed decision for access permission, the resounding answer from everyone has been yes," Wilson says.

Colorado is among states that have participated in pilot programs. Micheline Casey, director of identity management in the Colorado Governor's Office of Information Technology, says they plan to issue between 10,000 and 15,000 FRACs over the next two years in the north central region, which includes the Denver metropolitan area.

"I think that, overall, people are really enthusiastic," Ms. Casey says. "We are a rural state with most of the population in the Denver metropolitan area, so people tend to go across county boundaries to help each other out, and they don't always know everyone who shows up."

Colorado is looking at a variety of ways to apply the technology beyond use during a major incident; for example, access to buildings including jails and courthouses and access to computer systems and networks.

"FEMA is using the technology for ultimate worst case scenarios, but identity management is done the same way whether it's getting into a building, bank, your car or a disaster scene," Wilson says. "The key is to get everyone moving in the same direction. We are truly achieving robust interoperability that can be trusted."

Progress continues to be made at the federal HSPD-12 level. The General Services Administration's Managed Services Office (MSO) provides credentialing services to over 70 federal agencies, including the U.S. Department of Justice, according to Raymond Kimble of Excella Consulting, which supports the MSO. To date, approximately 400,000 people have been issued credentials through the MSO for identification and building access, and that number will eventually grow to 800,000 people.

For more information, contact Stephen Duncan, branch chief, GSA HSPD-12 Managed Services Office, at (703) 605-3492.

This article was reprinted from the Winter 2010 edition of *TechBeat,* the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center System, a program of the National Institute of Justice under Cooperative Agreement #2005–MU–CX–K077, awarded by the U.S. Department of Justice.