FIRST RESPONDER AUTHENTICATION Credential Solution

SOLUTION BRIEF

"Once FRAC is completely implemented, we will be able to efficiently track and deploy authorized personnel during crisis or emergency events, allowing us to better serve and protect the residents of Illinois."

—Director Larry G. Trent,
Illinois State Police.

Prior to 9/11 and Hurricane Katrina, comprehensive, unified plans for validating credentials during all-hazards event response and recovery efforts did not exist. The lack of a standardized identity verification system during disasters such as these reduced accountability for emergency personnel and hindered coordination efforts. Without a reliable means of authentication, it was difficult to determine who was already on site and what resources were available, often resulting in confusion, delays, vandalism, and theft. It was clear to emergency agencies and government officials that, in times of crisis, a secure and dependable method for identifying and managing those who are first on the scene was greatly needed.

The Illinois Terrorism Task Force (ITTF) set forth a major initiative to create the first statewide, interoperable identification and authentication plan that provides a common system for communicating among public safety officials during an emergency.

With the involvement of several different technologies and integration concerns, ITTF approached Entrust, CoreStreet, and SafeNet to create a common and reliable standardized identification verification system that fulfills government standards for interoperability between agencies.

Components of the ITTF Emergency Responder credential solution include personal identity verification (PIV) cards, public key infrastructures, hardware security modules (HSMs), middleware, card credential management systems, and physical access systems.

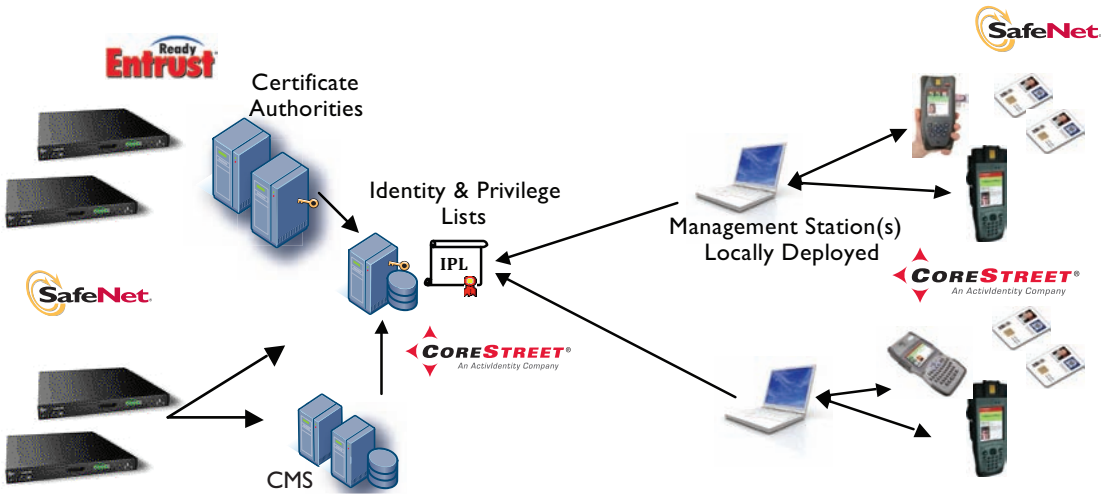
This solution enables specific organizations to use digital certificates for authentication, encryption, digital signatures, and physical and/or logical access, but without expensive upfront investments, in-house experts, or secure facilities.

How does it work?

With the use of digital identities provided by an Entrust PKI operated by the Illinois Department of Central Management Services, the ITTF Emergency Responder credential solution enables local, state, and federal agencies to confidently make access decisions at any incident by quickly authenticating and validating — via a SafeNet smart card and a CoreStreet Enabled™ handheld credential reader — the identities and roles of individuals wishing to enter or exit a secure or restricted area. Verified knowledge of roles, identities, and privileges enables agencies to manage emergency response officials and allows incident command to adjust quickly to emergencies by distributing personnel where they're needed most.

The ITTF Emergency Responder credential solution is FIPS 201-compatible and interoperable with numerous smart credentials issued by various government entities using Entrust PKI, and who's digital Identities are protected by SafeNet HSMs. Further interoperability comes through cross-certification with the U.S. Federal Bridge Certification Authority (FBCA), which allows credentials to be verified across federal, state, and local agencies, and among jurisdictions.

* "State and Local Agencies Comply with First Responder Authentication Credential (FRAC) Initiative." GSN's Essential Guide to Disaster Preparedness and Response Oct. 2008.



The Entrust certificate authority, operated by the State of Illinois provides and manages the digital identities assigned to first responders that are stored on the smart cards. These secure digital identities can be leveraged as the foundation of a layered security strategy designed to protect homeland security information, or can also be extended to enable other applications across the state enterprise.

CoreStreet offers an integrated solution consisting of an infrastructure component linking locally managed attributes to existing global identity management systems. The software for handheld devices is designed to allow authorized personnel the ability to control access to any site with confidence by quickly authenticating and validating the roles and identities of individuals requesting access. The CoreStreet PIVMAN solution is the only solution that is on the FIPS 201 Approved Products List, the DHS Authorized Equipment List (AEL) and the Standardized Equipment List (SEL). Products on AEL and SEL are 100% reimbursable through DHS grants.

SafeNet (FIPS 201) compliant HSMs protect the Federal and Corporate IDs together with the Entrust PKI and CoreSteet validation products, while its FIPS 201 compliant Smart Cards provide authentication, identity verification, trust, and privacy for both physical and logical access. SafeNet HSM and smart card technologies have always supported PKCS #11 and MS-CAPI interfaces, allowing for seamless integration and interoperability with applications and products from leading authentication and information security companies. Plus, by using your PIV-compliant credentials with other SafeNet security solutions, you can extend your security capabilities.

For more Information

www.entrust.com
Brent Crossland
(217) 341-7467

www.corestreet.com
Paul DeCrisantis
(860) 286-1081

www.safenet-inc.com
Mike Graff
(630) 983-0279