Emergency Response Official Credentials: An Approach to Attain Trust in Credentials across Multiple Jurisdictions for Disaster Response and Recovery

A Smart Card Alliance White Paper

Publication Date: October 2008

Publication Number: IC-08001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

Table of Contents

1 Introduction

Emergency response officials (EROs) require a means of identifying themselves and their abilities (skill sets and attributes) for daily access to work locations and sites during routine and emergency situations or special events. This need extends to all emergency response communities[1] and applies both in their local areas and across the nation, as EROs are asked to provide support during national disasters and other emergency situations that may not be in their local jurisdictions. There are strong drivers to move from a flash-pass and paper-laden environment to one that uses a machine-readable credential with a fast, secure electronic validation process that works in all environmental conditions, even when neither power nor communication capabilities are available.

Secure and trusted identification credentials achieve two goals. First, they enable EROs to perform day-to-day activities efficiently, by providing access to facilities, locations, and information. Second, they provide identity authentication with a high assurance level during emergency response and recovery activities. The need for identification credentials that can be used every day and also be leveraged in an emergency on "the" day has been highlighted by a number of high profile events, including the September 11 attacks and Hurricane Katrina. The lack of electronically verifiable credentials that could be trusted across multiple jurisdictions was a major problem identified in both the 9/11 and Katrina Congressional post-incident reports. Standards need to be established to enable multi-jurisdictional trust in credentials used by EROs, both now and in the future. To address this issue, this white paper presents an ERO credential model that is based on Federal Information Processing Standard 201 (FIPS 201).

For both daily activities and emergency situations for EROs, it is necessary to quickly and unequivocally establish who is requesting access and what the ERO is allowed to do based on their certified skill set (e.g., medical personnel, law enforcement officer, firefighter). Without the ability to identify and qualify individuals with a high level of assurance, the response and recovery effort can be compromised, affecting the economic and human impact and the ability to return to life as normal. The need to answer these two basic questions is a primary driver for the implementation of a secure and trusted identification credential for EROs and an efficient infrastructure to support and sustain the credentialing process.

Organizations are increasingly recognizing the benefits of using a single smart card-based credential for identity and attribute authentication that allows daily access to secure areas, facilities, and networks, and also grants access to emergency scenes or special events. These benefits include:

- Improved security and reduction in unauthorized network access through strong authentication, single point of revocation, and the ability to associate logical and physical access permissions
- Cost savings, such as a reduction in help desk calls and easier administration of physical and logical access systems
- The ability to create a single directory to administer users
- Greater efficiencies in using a single method for access across resources and, over time, across organizations
- Protection of the privacy of personal information stored on the credential
- Most importantly, the ability to trust, with a high level of assurance, that personnel who are permitted access into and movement within an incident area have been electronically validated as necessary to serve the restoration and recovery process

The benefits of a secure, trusted credential constitute additional motivation for organizations evaluating a move to smart card technology.

[1] Emergency response communities include the Federal Government; state, local, and tribal governments; volunteer organizations; and critical infrastructure organizations.

1.1 Identity Credentialing System Concepts

A few key concepts apply to all secure identity credentialing systems. This white paper uses the following terms:

- **Identity** is the subset of physical and/or behavioral characteristics by which an individual is uniquely recognizable. Identity is information *concerning* the person, not the actual person. In a credentialing system's identity vetting/proofing process, an individual presents documents (e.g., birth certificate, driver's license, passport) to verify identity; other information (e.g., biometrics) is collected to create an identity credential.
- An **attribute** is a qualification, certification, or skill set associated with an individual. For example, ERO attributes could be assigned according to the National Response Framework (NRF) Emergency Support Function (ESF) codes and/or the National Infrastructure Protection Plan (NIPP) sectors.
- An **identity credential** is the digital information that authoritatively binds an individual's identity (and, optionally, additional attributes) to that individual. The identity credential is typically stored on an identity card (e.g., a smart card).
- **Authentication** is the process of using an issued identity credential to validate the identity and/or attributes of a person or other entity electronically. For example, an ERO's identity and attributes can be authenticated prior to allowing access to an incident site by reading the ERO credential with handheld devices.
- A **privilege** is the authorization or right to be granted access to a controlled area or resource. Privileges are assigned to an individual based on that individual's identity and attributes. Access is permitted or denied based on assigned privileges. For example, once an ERO's identity has been authenticated, the local incident commander can grant the ERO privileges and authorize the ERO to access appropriate areas or resources.

Section 4 includes a description of an ERO credentialing system process and discusses how identity is verified and identity credentials are issued.

1.2 FIPS 201 and ERO Credentials

The goals for ERO credentials go hand in hand with the mandate established by Homeland Security Presidential Directive 12 (HSPD-12), which applies to employees and contractors of the Executive Branch of the Federal Government. Issued on August 27, 2004, this directive called out the need "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." The directive specifically calls for the use of a common identification credential for "gaining physical access to Federally-controlled facilities and logical access to Federally-controlled information systems."

As a result of this directive, the National Institute of Standards and Technology (NIST) published FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, initially issued on February 25, 2005 and updated to FIPS 201-1 in March 2006. FIPS 201 defines the identity vetting, enrollment, and issuance requirements for the identity credential, as well as the technical specifications for the PIV card.

The FIPS 201 PIV card is a dual-interface smart card that is being issued to all Federal Executive Branch employees and contractors. The contact interface is typically used for logical access control and the contactless interface for physical access. The card can also be used for other applications, such as payment, transit, and issuance of equipment.

FIPS 201 provides a set of technical standards and policies that can be leveraged to provide secure ERO identification credentials. An ERO credential that is technically compatible and interoperable[2] with FIPS

[2] *PIV compatible* cards meet the FIPS 201 technical specifications so that PIV infrastructure elements such as card readers are capable of working with the cards. However, the credentials are not issued in a way that assures they

201 will help establish and verify identity and link identity with attributes electronically, facilitating management of EROs during incidents and special events. The credential can also support a number of physical access use cases, from allowing site controllers to make command decisions based on trusted information to enabling individuals to use the credentials for equipment management. For an ERO credential to be used in these scenarios, the credential must conform to a common trust model. This model must rely on common processes for vetting, enrollment, issuance, attribute management, and training, and also provide the ability to audit compliance with these processes so that the trust model is established among ERO credential issuers.

The ERO credentialing process must ensure that claimed certifications meet minimum standards and that fraud is actively deterred. For example, consistent identity screening for all EROs ensures that employees, volunteers, and others are not on the terrorist watch list. The ERO credential can be used to establish a common chain of trust among jurisdictions, command personnel, and responders and also be used in other ways at an incident and in daily practice.

The Department of Homeland Security (DHS) is developing additional specifications and core attributes (certified skill sets) for use with EROs. These specifications will outline minimum training, trusted sources of information, and a means of documenting, updating, and revoking attributes. Local regions will then be able to integrate and manage these attributes in their own disaster response plans and systems. Most importantly, the attributes will be linked to ERO credentials, so that secure identification and electronic attribute authentication can be used for informed decision-making (for example, whether an ERO should be allowed access to a particular area during an emergency). DHS is also developing guidelines for ERO identity vetting that would provide non-Federal issuing organizations with a standardized, robust process to verify an individual's identity prior to credential issuance.

Implementing ERO credentials that function nationwide requires use of a common technology platform. Fortunately, the FIPS 201 standard supports this requirement. A growing number of General Services Administration (GSA) FIPS 201-approved vendors of logical, physical, and mobile devices have developed products built on FIPS 201 and industry standards for smart cards, digital certificates, and public key infrastructure (PKI). FIPS 201 has also attracted international attention and is under consideration for use by public safety and critical infrastructure personnel in other countries. Within the next five years, 12 million[3] PIV cards will be in use in the Federal Government alone, driving a significant increase in FIPS 201 infrastructure and applications. FIPS 201 provides a sound technology foundation for secure ERO credentials.

The Federal Emergency Management Agency (FEMA) is required by H.R. 1[4] to implement an infrastructure capable of supporting much of the ERO community in the United States. Setting a credentialing and typing standard that will enable trust and interoperability of identity and ERO roles is a requirement. The use of a standard such as FIPS 201 enables the trust environment that is desired to address the needs of the 9/11 and Katrina post-incident reports. For this reason, and to achieve the benefits cited above, FIPS 201 credentials should be the *de facto* foundation for an ERO credential.

This white paper was developed by the Smart Card Alliance Identity Council and Physical Access Council after discussion with DHS personnel to understand the complexities of trusting identity credentials at disaster response and recovery scenes. The Smart Card Alliance offers an independent assessment of how technology and processes can support achieving a high level of assurance in the identity of resources on hand to enable rapid decision-making by incident scene commanders on both a local and national scale.

---

are trustworthy by Federal relying parties. *PIV interoperable* cards meet the FIPS 201 technical standards, work with PIV infrastructure elements such as card readers, and are issued in a way that allows Federal relying parties to trust them. (Source: *Interoperability Parameters for Trusting non-Federal Identity Cards*, Judith Spencer, Inter-agency Advisory Board presentation, June 2008)

[3] Figure provided by the General Services Administration.

[4] "H.R. 1: Implementing Recommendations of the 9/11 Commission Act of 2007," introduced into Congress January 5, 2007 and signed into law on August 3, 2007. H.R. 1, Title IV, "Strengthening Use of the Incident Command System," Section 408 describes requirements and timelines for FEMA credentialing and typing of emergency response and critical infrastructure personnel.

2 ERO Credentials: Use Cases

This section reviews use cases for ERO credentials that take advantage of the standards and investment that result from FIPS 201. This investment not only includes government investment in the supporting infrastructure but also the very significant vendor community investment in the development of numerous interoperable and commercially available products. The foundation for all of the use cases is a smart card-based ERO credential that adheres technically to the FIPS 201 standard and, as a result, supports a wide range of applications.

To some extent, the range of applications supported depends on the credential profile and the certificates provisioned on the credential. Since, in most cases, the companies that are providing the credentials do not charge for individual certificates but have one fixed price for the credential, it is assumed (and strongly suggested) that the credential contain all four of the available FIPS 201 certificates: PIV Authentication, Card Authentication, Signature, and Encryption.

The power of a FIPS 201-based ERO credential is its ability to support both emergency and incident use cases and everyday use for other applications. At a high level, all applications fall into the category of access control. Access control applications answer two questions: "who are you?" and "what are you allowed to do?" The FIPS 201-based ERO credential provides a basis for answering the first question at a very high level of assurance. The ability to answer the second question depends on whether the associated infrastructure is federal, state, local, or enterprise.

The following sections describe how a FIPS 201-based ERO credential can be used for a wide variety of daily uses, including:

- Identity and attribute management (section 2.1)
- Emergency response (section 2.2), including incident scene access (section 2.2.2) and incident scene tracking (section 2.2.3)
- Physical access to facilities (section 2.3)
- Inventory control and equipment access (sections 2.3 and 2.7)
- Continuity of operations and emergency operations center (EOC) access (section 2.4)
- Logical access to networks and information systems (section 2.5)
- Mobile command centers (section 2.5)
- Secure email communications (section 2.6)
- Keyless access to vehicles (section 2.7)
- Public transit (section 2.7)
- Law enforcement status checks (section 2.7)

Appendix A describes recent demonstrations and pilots of ERO programs that implemented and tested different use cases for a FIPS 201-based ERO credentialing system.

2.1 Identity and Attribute Management

Knowing the identity and attributes of an individual with some level of assurance is required for most security deployments and electronic commerce. FIPS-201-based smart card security ties an individual's identity and attributes to the credential, which can then be used as a key element in many security- and commerce-related activities. When an identity is bound to a credential and attributes are associated with it, many potential applications can use them (as explained in the specific use cases in the following sections).

Establishing a common credentialing platform allows for centralized management of credential holders' electronic identities and attributes, creating benefits of scale and reducing redundant processes. For example, state and local governments can leverage the credentialing process as part of their current suitability and on-boarding processes. The credential itself can be used for both day-to-day activities (e.g., physical access to facilities and logical access to computers and networks) and emergency response. This multi-use approach helps build return on investment by reducing organizational spending on multiple identity management infrastructure solutions. Using a central source for identity also allows a single infrastructure to be leveraged across organizations and applications. In addition, using one

credential as a clearinghouse for attributes, training, and other personnel data facilitates attribute management.

Building multiple functions around a single identity platform, rather than creating additional credentials for each use case, can also result in personnel efficiencies. Credential holders must remember only a single personal identification number (PIN) rather than multiple passwords for logical access. A credential used for daily activities is more likely to be in an ERO's wallet than at home on a dresser when an emergency strikes. Daily use also means that PINs can be recalled more easily, and individuals will know which fingerprints are required for authentication when challenged at an incident perimeter.

If a high assurance identity credential is used as the platform for most daily activities, the chances for fraud are reduced, since the need for less secure credentials is eliminated. Also, credential holders will be less likely to attempt to bypass secure processes by displaying a lower assurance credential if fewer such credentials are issued.

2.2 Emergency Response

The value of having inherent trust in the identity and vetted attributes of people on an emergency response scene has been demonstrated by the problems encountered in controlling personnel during cross-jurisdictional disasters. Issues with unauthorized personnel accessing incident sites and authorized personnel being denied access due to the lack of verified identity credentials were reported from both the 9/11 and Katrina recovery efforts.[5]

A primary business driver for implementing ERO credentials is the establishment of a common means to validate electronically the identity and attributes of EROs arriving at an incident, so that proper access privileges can be granted. The benefits of using pre-issued, trusted, and interoperable credentials linked to attributes include:

- Fast identification of individuals and their capabilities, using an efficient, objective, and standardized electronic process
- Incident scene access permissions that are based on electronic identity authentication and defined trusted attributes
- Management and tracking of human resources, especially those with critical attributes, at an incident scene
- Provision of records for personnel who respond to an incident for post-event reconstruction and liability issue assessment

These benefits support two key components of incident response: access control and situational awareness. Both become particularly important when mutual aid is provided by members of communities outside of a particular location (the case where not everyone knows everybody else).

2.2.1 High Assurance and Trusted Identity

One of the critical lessons learned from 9/11, which has been reinforced by later emergencies such as Hurricane Katrina, is that it is difficult and time-consuming to confirm, with a high level of assurance, that people are who they say they are. Today Federal EROs (F/EROs) are able to address this need by using their FIPS 201 PIV credentials; other state and local EROs are using the FIPS 201 model and the First Responder Authentication Credential (FRAC) card.[6]

Using a FIPS 201 credential achieves high assurance by tying the individual's digital identity to a credential that uses the strongest available cryptographic techniques for identity protection and follows FIPS 201 identity vetting and issuance processes. In addition to using PKI, a FIPS 201 credential makes available up to four factors of authentication (PKI certificate, PIN, fingerprint, and digitally-signed

[5] "Mission Critical," http://www.tvworldwide.com/events/mission_critical/061018/default.cfm?id=7523&type=wmhigh

[6] See Appendix A for additional details on ERO demonstrations.

photograph), providing very high assurance (according to categories defined by NIST[7]). High assurance is also obtained by following the identity credential issuance process defined in FIPS 201.

In a high assurance scenario, individuals arriving at an incident site can put their credentials into a device running software that challenges each individual for a PIN, fingerprint, and/or photograph, and matches the results to information stored on the credential. The software also checks to see whether the credential is still valid.

As a result of being able to establish an ERO's identity unequivocally, FEMA and other organizations, such as the Department of Defense (DoD), have begun to implement an infrastructure that allows an individual's attributes (e.g., doctor, nurse, emergency medical technician [EMT], firefighter) to be associated with the verifiable identity of an F/ERO. The combination of high assurance identity and attributes allows rapid proof of identity, providing incident command staff with the ability to make better decisions about granting authorization for an individual to proceed with response and recovery efforts. Furthermore, the FEMA and DoD infrastructure is configured to enable this validation to occur in all environmental conditions, including times when power and wide area network communications have been lost. This capability has been verified in many demonstrations, which have included communities from Federal, state, and local governments, volunteers, and the private sector.

High assurance identity has many other applications in enterprises for logical, physical, and device access control. Finally, using a shared service provider cross-certified to the Federal identity infrastructure means that not only can a single organization's credentials be trusted, but any FIPS 201 or other cross-certified credential can be trusted. This results in credential interoperability across multiple jurisdictions and organizations.

2.2.2 Incident Scene Access

Managing cross-jurisdictional response teams requires tight control over who is allowed on the scene. Two steps are necessary to ensure that the right people enter the scene: requesting the right resources, and checking people as they enter the scene. In some regions, progress has been made toward creating regional resource programs that allow such requests to be made. ERO credentials can be linked to these programs while maintaining the core functions of electronically authenticating identity and defining attributes. Encouraging local entities to populate ERO credential information can help in determining the availability of local resources, requesting resources, and quickly reviewing resource status in the region as necessary.

Once they arrive on scene, ERO credential holders (who can include employees or contractors) can be logged in to the system. Their presence can be validated against the request (number and identities of people) and their claimed identities and attributes can be validated by electronically reading the ERO credential. Electronic authentication is performed using secure multi-factor authentication over the contact interface and can include up to four factors (PKI certificate, PIN, biometric, digital photograph). The ERO credential can also be checked for revocation status (to determine whether it is valid) and for the individual's attributes (to determine the individual's role). Attributes are typically assigned according to the NRF ESF codes or the NIPP sectors, or both.[8] These identify, at a high level, the individual's role and ability to respond to an incident, laying the groundwork for enhanced situational awareness.

A screening application can also keep track of the number and types of individuals who have responded to an emergency, match them against requested resources, and share this information by aggregating data from handheld authentication device software on a device management station. FEMA and the Pentagon Force Protection Agency (PFPA) have implemented this type of infrastructure in the National

[7] NIST Draft Special Publication, SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS).*

[8] See Appendix B for the definition of the ESF codes and NIPP sectors.

Capital Region (NCR). This infrastructure leverages the ERO credential by providing a means for associating privileges with an individual and a credential. In other parts of the country, this infrastructure is being established at the state level.

Handheld readers can be used (offline) to read the credentials of those within a scene and at access points and validate attributes and identities against a pre-defined list. It is important to note that identity and privilege checking must be supported without any network connectivity by using a device that has previously been synchronized with this information so that current information is available. Synchronization scheduling is set at a local level and is typically between 24 and 48 hours. When an event requires hundreds or thousands of EROs within a perimeter, checkpoints or mobile check units can be deployed to update resource locations rather than validate identities. Electronic credentials can also be read to record who exits from a scene, enabling post-event reconstruction; this "exit logging" can be streamlined using the contactless credential interface.

2.2.3 Situational Awareness and Incident Scene Management and Tracking

In incidents of limited scope, site commanders will typically know what units are requested for a particular event and will only allow requested individuals past the perimeter. However, in a widespread incident, perimeters may be porous or established when people are already inside. An incident may be too big for a single command post to manage all requested units. Additionally, incidents at high security facilities may require concentric perimeters with different access controls. In these instances, ERO credentials are critical to ensure accurate validation of the identities, attributes, and locations of both individuals who are within the site and individuals who are requesting access to the site.

Information read electronically from an ERO credential can be used for incident scene management and for tracking. Firefighters who commonly use Velcro boards to track the location of people at a scene could instead use an electronic map application that is updated each time an ERO credential is read by any reader (entrance, egress, or roaming in-site scans). Such use facilitates accurate accounting of people within established perimeters.

During a typical incident, a site commander will request support from various attribute holders (e.g., EMT, search and rescue, bomb squad). If conditions change, having a list of all personnel on site, their associated attributes, and their approximate locations allows new teams to be formed easily and quickly on the basis of needed capabilities. In addition, reading an ERO's credential can electronically validate whether the individual has the appropriate attributes to cross a perimeter or perform a particular duty.

Auto-logging, a function that can store information about entry and egress of people and assets, can also be added to an ERO access system. The benefits of auto-logging personnel movement at a scene include personnel safety after an incident is over and improved response plans. For example, people exposed to an area that is determined to be hazardous after the fact can quickly be notified to seek proper treatment (during post event reconstruction). Also, proof of access to an area may eliminate potential lawsuits over health coverage (like those that are currently occurring in New York City, since no proof exists that an ERO was exposed to the health hazards at Ground Zero). Metrics can also be evaluated against results to pinpoint areas of failure and create actionable lessons learned.

2.2.4 Just-in-Time Credentials

Any resources without a pre-issued ERO credential can be issued just-in-time credentials on site. These credentials could be technically interoperable with the FIPS 201-based ERO credentials but without the same level of trust in the vetting of the individual's identity. Just-in-time credentials could be visually and technically distinguishable from a FIPS 201-interoperable ERO credential and not allow users to access sensitive or secure areas of a site. Eligibility could be restricted to certain populations only, such as Red Cross personnel, and then only with particular proof of identity. Vetting could require that the applicant

produce a passport, a Transportation Worker Identification Credential (TWIC), FRAC, or other secure document that has been established as suitable for identity proofing. Attributes can be added to the just-in-time credential based on training programs completed at the command post or valid proof of ability (e.g., EMT credentials).

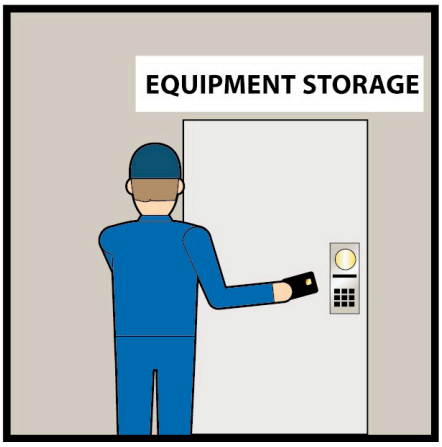
In addition, EROs may be able to use other Federal or state credentials that have been determined to be acceptable at the incident site (e.g., TWIC or DoD Common Access Card [CAC]) and that associate the appropriate attributes with the credential holder.

2.3 Physical Access to Facilities

Since a FIPS 201-based ERO credential is based on smart card technology, it can be integrated with other common radio frequency (RF) and smart card applications. Some common daily uses could include:

- Allowing access to facilities within the ERO's home jurisdiction, providing return on investment if the ERO credential is used as the primary identification credential or building pass
- Authenticating identity for access to secure facilities owned and operated by multiple entities
- Establishing inventory control

The most common application would be for the ERO credential to be used as a pass to enter secure facilities. Since the credential can have both RF and computing capabilities, it could be used to standardize and centralize all physical access control systems (PACS) in a region. For example, sheriffs could use their ERO credentials to enter the secure areas in all regional courthouses, once their identity and attributes have been electronically validated and access privileges have been granted.



During an incident, it is very likely that certain EROs will need physical access to equipment storage locations, key operational buildings and facilities, and, in some cases, municipal buildings that are secured with access control readers and card-reader controlled access points. Gaining access to these assets may require enrolling EROs in the controlling PACS and issuing them facility-specific passes, which is not always practical in emergency situations. The interoperability of the ERO credential and its basis in smart card technology could allow identified access control systems to be provisioned with formats that are compatible with the ERO credential, allowing EROs to access such facilities more easily.

A variety of technologies supported by the FIPS 201-based ERO credential can be used to enable this functionality. Since FIPS 201 has become a standard within the Federal government, all card readers in these facilities will soon be able to read the short-range contactless interface of the ERO credential. ERO credentials will be able to interoperate with any of the readers on the GSA Approved Products List (APL)[9]. In addition, the topologies supported by FIPS 201 credentials include 1-D and 2-D barcodes, magnetic stripes, and traditional proximity chips. FIPS 201 data models have also been proven to work with biometrics, such as fingerprints, iris scans, and hand geometry, all of which are common at access points.

Of course, a PACS must be configured with information that enables the system to recognize ERO credentials; this is the so-called provisioning process, which can be completed in a variety of ways. Provisioning can be accomplished before an incident or only as needed after an incident has already occurred. A variety of techniques can be used; some streamlined approaches may require development of a supporting infrastructure, but manual processes can be used with minimal technical upgrades.[10]

[9] The GSA APL can be found at http://www.idmanagement.gov.

[10] The Smart Card Alliance white paper, "Considerations for the Migration of Existing Physical Access Systems to Achieve FIPS 201 Compatibility," provides guidelines for how to assess current PACS capabilities and migrate to

2.4 Continuity of Operations and Emergency Operations Center Access

A related but slightly different use case for ERO credentials involves continuity of operations (COOP) or continuity of government (COG). In this case, an individual's attribute is designated as part of the continuity team and the individual typically needs to access an emergency operations center (EOC) or relocation site. The ERO credential may be used to electronically authenticate the identity and attributes of the individual accessing the EOC or to provide the individual with transportation to the EOC or relocation site in addition to access to the facility itself. People from across an enterprise and from other enterprises typically use an EOC's high security facilities. The ERO credential vetting process, credential use, and mobile capability for electronic authentication and authorization provide a means to ensure that the right people get to their EOC quickly.

The relocation use case is typically supported by a handheld reader running validation software in the same manner as the emergency response application (authentication, revocation check, attribute/privilege check), while facility access is typically supported through the PACS.

This use case requires the strongest possible authentication at the highest level of assurance. Software in handheld readers is currently available that can deliver strong (up to four-factor) authentication and a specific assignment of COOP privileges. Numerous Federal agencies are in the process of implementing this approach.

The initial deployments of ERO credentials in the NCR have focused on COOP for the Federal government. These efforts are being complemented by those who are responsible for critical infrastructure in the NCR (e.g., telecommunications, utilities and financial services workers, among others) who can leverage the infrastructure being put in place by FEMA.

Critical infrastructure providers can issue a FIPS 201-based ERO credential to their employees and register their staff in the particular NIPP sector along with their COOP responsibility as attributes. Critical infrastructure personnel with these credentials will be able to cross boundaries and checkpoints in emergencies. This use case has the ability to drive wider adoption of FIPS 201 ERO credentials in private sector organizations.

In addition, organizations operating EOC facilities can leverage the validation infrastructure and FIPS 201-based ERO credentials issued with the appropriate ESFs to determine whether multi-jurisdictional public safety, fire, emergency medical technicians and others responding with mutual aid to their facilities really are who they say they are and have the appropriate ESFs to meet the particular need at their facilities (e.g., put out a fire, detain individuals, provide medical assistance).

2.5 Logical Access to Networks and Information Systems

A FIPS 201-based ERO credential can support a wide range of logical access control applications (applications providing secure access to networks and computers). The credential can be used for daily logical access for those organizations with a need for strong authentication and encryption. This will certainly be the case for any ERO who is part of the Federal government.

Examples of logical access control applications include:

- EROs electronically authenticating their identities to access computers and networks where emergency information is shared with state and local groups as well as with Federal ERO groups. In many cases, this will be accomplished through web sites and other computer-based

be compatible with FIPS 201 credentials. The white paper is available at http://www.smartcardalliance.org/pages/activities-councils-physical-access.

communications

- EROs accessing the names of casualties, the location and status of COOP (or government) personnel (including VIPs), resource allocation, and other instructions and information from a secure a web site.

Daily use of a FIPS 201-based ERO credential can become a common practice, as it is already in the DoD. Information sharing is crucial during an emergency, and the ability of a smart card-based ERO credential to support logical access control meets this need.

In many disaster scenarios, a mobile command center is the information hub of the incident area and is designed for rapid deployment and activation. These centers often house computers, laptops, and, in large-scale relief efforts, server racks. Operators, incident commanders, and EROs in the field use these and other devices, such as handheld smart card readers and other mobile electronic devices, to share information with each other and with people who are outside of the immediate area (e.g., staff at a regional headquarters or EOC). There are three lines of defense for logical access and secure communication transmissions: authentication to machines, secure point-to-point communications channels, and authentication to web sites. All of these defenses can be accomplished easily, and with the highest level of security, using the FIPS 201-based ERO credential.

Access begins with device authentication by smart card device logon. Device authentication is accomplished by leveraging any combination of PIN, fingerprint match, and digital certificate (the part of a PKI that stays on a credential). Logon requirements are easily managed with standard computers, as most laptops now have built-in card readers, and operating systems provide support for smart card logon. Credentials must be checked to determine whether they are in good standing, which is done by looking up the credential's revocation status. Credential checks can be managed using online links to the certificate issuer or by consolidating lists that can be checked when the reader is offline.

After a user has authenticated to a device to which the user has privileges, the user can opt to set up a secure transmission channel. Setup is achieved by establishing a virtual private network (VPN) using a combination of local and host software and a suitable logon. The FIPS 201-based ERO credential can provide certificates for logon, and sessions can be terminated immediately when the credential is removed. Establishing a VPN is useful for command posts that are in constant contact with regional headquarters or other posts to ensure that critical information is not intercepted.

Smart card logon also facilitates establishment of secure web site access. This access uses the PIV Authentication Certificate in much the same way as smart card logon and VPN establishment. In this case, the browser and web server need to support certificate-based authentication, which are common components of most commercial systems. In one example of a highly secure website, DHS operates a Homeland Security Information Network (HSIN). The HSIN site has a confidential area; access to HSIN could be a commonplace use of the FIPS 201-based ERO credential.

The above scenarios are not only applicable to logical access during incident response, they are also applicable to daily activities. Local responder organizations that have information to protect can use their credentials to establish a coherent information management program. In any scenario, the logical access applications must be provisioned with credential information.

2.6 Digitally-Signed E-mail Communications

An e-mail message can be digitally signed so that the recipient knows that the message has not been modified and has come from a particular individual. E-mail messages can include requests for information or material, directions, orders, status reports, and other types of signed documents. If the full suite of FIPS 201 certificates is used, e-mail messages can be encrypted as well as signed. Digitally signed e-mail messages provide the ability to maintain communication secrecy, nonrepudiation of content, and identification of the sender.

Digitally signed e-mail communications would be used the same way in an emergency response scenario as in any enterprise. To support this functionality, an organization can leverage a wide range of products that support digital signatures. Most e-mail client applications support the use of digital certificates.

2.7 Other Use Cases

The flexibility inherent in the use of a smart card as an ERO credential allows for additional use cases. For example, the ERO credential could be used to check out equipment and keep a record for audit purposes. Personnel could sign for equipment using the ERO credential, and the system could track entry to storage lockers and match equipment tags to the ERO credential holder who requested the equipment. The ERO credential could also be used for keyless access to shared vehicles; in this application, the ERO credential would both serve as a key and create an audit trail.

Other use cases may be specific to certain regions, such as use for public transit or identity checks during traffic stops. For example, public transit agencies in some locations have smart card payment systems; these applications could be added to the ERO credential. Regions with a high volume of plainclothes police or traffic routes with many off-duty police (e.g., populations that may legitimately be carrying weapons) could use ERO credential validation to check law enforcement status. In this use case, an officer would have more than a generic badge to validate armed drivers during traffic stops. Validation of this nature depends on trusting both the identity and the assigned attributes on the credential.

3 ERO Credentials: Benefits of Using FIPS 201 and Smart Cards

FIPS 201 radically changed credentialing in the Federal government by defining both processes and technical specifications for high assurance, interoperable identity credentials. The standard has had far-reaching effects—both within the Federal government and in enterprises and state and local governments—as organizations recognize the benefits of FIPS 201 smart card-based identity credentials. These benefits include:

- Interoperability
- Strong authentication, driving higher security, improved efficiency, and reduced costs
- Credential security
- Information privacy
- Support for multiple applications
- Standards-based credentials

3.1 Interoperability

Because FIPS 201-based products are based on publicly available, well-defined standards, interoperability is a key feature of certified cards and certified card reader technology. Certified cards and certified card readers are guaranteed to be able to read and process data encoded on the card by different organizations using equipment and software from different manufacturers. FIPS 201-approved products and services are listed in the GSA APL at http://www.idmanagement.gov/.

Of critical importance to the ERO community is the ability to read and verify credentials issued by municipalities, state entities, federal entities, volunteer organizations, and critical infrastructure providers. Using Hurricane Katrina as an example, properly securing the disaster area and assuring that the right services were delivered by the right individuals with the right skill sets at the right time required identifying the persons who presented themselves. An interoperable credential that can be authenticated electronically and that can securely validate the identity of the credential holder provides a means of getting the right services to the right people quickly. The interoperability of a FIPS 201-based credential makes it the logical choice for the ERO community.

FIPS 201 also provides a basis for trusting the credential issuance process. The combination of a strong authentication credential leveraging a cross-certified and federated PKI and a common enrollment, registration, and issuance process results in the trust required for interoperability. It is critical to understand the difference between compatibility and interoperability and the associated benefits.

Compatibility provides the benefit of being able to use the growing range of products on the FIPS 201 APL. Cards, readers, software, and other products can be purchased from a variety of vendors and can be connected and function as a system. FIPS 201-compatible credentials meet the technical specifications of the standard but are not issued in a way that provides assurance that they are trustworthy by Federal relying parties.

Interoperability focuses on trust and a means of establishing it. The implementation of HSPD-12 and FIPS 201 is establishing a community of more than 10 million credentialed government employees and contractors. Federal agencies accepting FIPS 201 PIV credentials can trust that other Federal issuing organizations have gone through a secure issuance process, that the facilities where their secrets are housed meet assurance and availability standards, and that there is an unequivocal means of determining that the credential is valid. ERO credentials based on FIPS 201 will also be interoperable with the infrastructure being put in place to support the government-wide employee and contractor credentialing efforts. Interoperability ensures compatibility, but compatibility alone does not ensure interoperability.

DHS and FEMA are working with the American National Standards Institute (ANSI) to develop specifications for ERO credentials that would allow these credentials to be used compatibly and interoperably across the United States.

3.2 Strong Authentication

A FIPS 201-based ERO credential provides very strong authentication and a high level of trust. A number of recent publications have highlighted the benefits of strong authentication.[11] Using a FIPS 201 credential would allow EROs, their organizations, and those organizations with whom they collaborate to achieve the highest possible identity assurance across a wide range of transactions. Strong authentication, built on strong identity assurance, provides the highest possible confidence that the person about to log in, go through a door, or respond to an incident scene is who they say they are and provides a strong basis for further authorizations. As important in the ERO credential and FIPS 201 model, there is a standard among organizations for achieving high assurance and system interoperability at this level.

Recent publications have developed a long list of the benefits of strong authentication, of using a certificate-based smart card to achieve strong authentication, and of using the FIPS 201 model. These benefits fall into three categories: security, efficiency, and reduced costs. (Additional information on these benefits can be found in the reports referenced below.)

Security benefits accrue across the board. The overall increase in an organization's security profile makes fraudulent access more difficult and reduces the risk of inappropriate access to sensitive locations and information. Strong authentication enables security personnel and scene commanders to make objective decisions about personnel identities and attributes that are based on electronic identification. Counterfeiting a FIPS 201 credential is effectively impossible, so decisions based on its information become straightforward. Strong electronic authentication provides additional benefits such as more efficient administration (including enabling the ability to revoke an individual's logical and physical access privileges with one action, if supported by the organization's policies) and better security audit trails, both for real-time monitoring and forensic security activities. The technologies that enable strong identity assurance also provide strong protection against fraud and identity theft. Anti-counterfeiting features mean that identity credentials cannot be cloned; global revocation means that lost credentials are easily disabled.

Efficiency benefits include faster access to computer networks, improved ease of use for users (they need to rely on only a single credential), easier network and access control administration (only a single credential is required), easier remote logon for a mobile work force, and the ability to support single sign-on to web sites and other applications.

Cost savings and economic benefits have continued to increase as organizations deploy smart cards and FIPS 201 credentials. These benefits include reduced help desk costs associated with resetting passwords, an overall reduction in the administrative costs associated with identity management and access control, and time savings across organizations due to more efficient identity administration. The lifecycle costs for other strong authentication methods (such as one-time password tokens) are substantially higher than the cost of smart cards. Cost savings result from having to deal with only a single credential for logical and physical access. The use of strong authentication can even lower insurance risk premiums.

3.3 Credential Security

Smart card-based ERO credentials are highly secure, protecting both the information that is on the card and assuring that the card itself is authentic.

[11] For more information on the benefits of strong authentication, see the following publications:

- "A new look at the ROI for enterprise smart cards: the value of converged access, SSO and remote access solutions," *Datamonitor*, January 2008
- "Strong User Authentication: Best in class performance at assuring identities," *Aberdeen*, March 2008;
- "Logical/Physical Security Convergence: Is It in the Cards?" *Aberdeen*, December 2007
- "Trusting the Team: Identity Protection and Management," *CrossTalk*, July 2007 (http://www.stsc.hill.af.mil/crosstalk/2007/07/0707DIAP.html)

Protecting the authenticity and integrity of the data encoded on the ERO credential is a primary requirement. When using smart card technology, sensitive data is typically encrypted, both on the credential and during communications with an external reader. Digital signatures can be used to ensure data integrity, with multiple signatures required if different authorities create the data. To ensure privacy, applications and data on the credential must be designed to prevent information sharing.

When compared with other tamper-resistant identity credential technologies, smart cards represent the best compromise between security and cost. When used with other technologies such as public key cryptography and biometrics, smart cards are almost impossible to duplicate or forge, and data stored in the chip cannot be modified without proper authorization (a PIN, biometric authentication, or cryptographic access key).

Smart cards also help deter counterfeiting and thwart tampering. Smart cards include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks. In situations where smart ID credentials are used to verify identity manually, visual security features can be added to the card body.

3.4 Information Privacy

The use of smart card technology for ERO credentials strengthens the ability of the credentialing system to protect the privacy of personal information.[12] Unlike other identification technologies, smart cards can implement a personal firewall for an individual, releasing only the information required and only when it is required. The smart card's unique ability to verify the authority of the information requestor and its strong card and data security make the card an excellent guardian of the credential holder's personal information. By allowing only authorized, authenticated access to the information required for a transaction, a smart card-based ERO system can protect an individual's privacy while ensuring that the individual is properly identified.

3.5 Support for Multiple Applications

The trend in smart card use has been to allow multiple applications to reside on a single smart card. Hosting multiple applications on a single card has numerous advantages, including cost benefits (the cost of the card is shared by all applications) and convenience (credential holders can use their credentials for multiple purposes, increasing the overall value of the card).

Within the Federal Government, the FIPS 201 PIV card is used for both physical and logical access to Federal facilities and can support other applications as defined and required by individual agencies. As described in the use cases in Section 2, smart card-based ERO credentials can support a variety of applications, including electronic identity and attribute validation at incident scenes, physical access to facilities, logon to networks and computers, and secure authentication to online information and during online communications.

3.6 Standards-Based Credentials

Smart card technology is based on mature international standards. Cards and readers complying with these standards are developed commercially and have an established market presence. Over 4.4 billion smart cards were shipped in 2007[13] and are being used worldwide in identity, payment, healthcare, transportation, and telecommunications applications. Multiple vendors are capable of supplying the standards-based components necessary to implement a smart card-based identity credentialing system, providing buyers with interoperable equipment and technology at a competitive cost.

FIPS 201 goes a step farther, providing an industry standard for products that support strong identity authentication. The Federal Government's commitment to FIPS 201 is driving the availability of a wide

[12] For additional information on how smart cards can enhance privacy in an ID system, see the Smart Card Alliance white paper, "Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology," available at www.smartcardalliance.org.

[13] Source: Eurosmart, http://www.eurosmart.com/4-Documents/Figures07ShipGlobal.htm

variety of smart card products and support systems (e.g., operating systems, physical access systems) that conform to the standard. For example, GSA maintains an APL for FIPS 201-compliant products and services and both GSA and NIST offer services that test compliance to the standard.

As a result, the infrastructure components needed to implement a strong identity authentication program are readily available. Multiple vendors offer interoperable equipment and technology at competitive prices with significant economies of scale.

In addition, the FIPS 201 standard supports other identification technologies (e.g., magnetic stripe, bar code, contactless/radio frequency). Issuers therefore have options for credentialing those members of the emergency response population who do not need a full-featured ERO credential and for compatibility with legacy systems.

4 Smart Card-Based ERO Credentialing System Process

For a smart card-based ERO credentialing system to be both effective and secure, a complete set of system processes must be followed consistently. This common platform of secure and standard practices enables trust among the different issuers of ERO credentials. The process is composed of several steps, as illustrated in Figure 1.

- **Sponsorship**. A sponsor's duty is to vouch that an applicant has a need for an ERO credential and authorize applicant enrollment. The sponsor may also authorize the cost incurred for the credentialing process.
- **Enrollment**. The enrollment process is designed to verify the identity of an applicant in person and collect information from the applicant. Applicants must bring two forms of identification and are fingerprinted and photographed at enrollment. The information collected is used to perform suitability checks and to create the credential.
- **Adjudication**. Trusted adjudicators determine whether an applicant can receive a credential based on the results of the suitability check. Identity vetting procedures (e.g., National Agency Check–with Inquiries [NAC-I], education, employment, credit history, and verification of claimed skills) are part of the adjudication process, with disqualifiers defined as part of the vetting procedures. Passing adjudication successfully triggers credential production.
- **Credential production**. Credentials can be personalized in a centralized facility or at local issuance stations. Relevant information is printed according to Federal standards, security features are added, and the electronic smart card chip is encoded with personal data.
- **Issuance and activation**. When an applicant arrives to pick up the personalized credential, the issuer verifies the applicant's identity by reverifying the identity documents presented at enrollment and matching the applicant's fingerprint to the one used to enroll. The credential is then "unlocked," digital certificates and a PIN are loaded onto the chip, and the credential is released to the applicant for use.
- **Credential use**. Activated credentials can be used to access secure physical locations and computer networks and to validate identity and attributes electronically at incident sites. The digital certificate can be verified through handheld devices to authorize access to incident sites.

All of these process steps must be supported by both technology and policies and procedures. Only the consistent execution and enforcement of policies and procedures can ensure the overall integrity of the system.

In addition to these core identity system processes, ERO credentials will also be used to help manage attributes (such as law enforcement officer, EMT, or other relevant data). These attributes are currently being defined, can be added to a credential holder's record during or after enrollment, and can be updated locally. DHS is currently devising a technology architecture to collect this data and link it to an ERO credential.

Managing credentials over their life cycle has equal importance to issuance and specific credential use cases. Both attributes and certificate revocation status must be managed over the credential lifecycle.

Local organizations, whether involved in public safety, fire, or emergency medical response, will need to manage the ERO's **attributes**. These local organizations will keep the status of ERO attributes up-to-date and provide attribute status updates to the FEMA infrastructure.

Certificate revocation (independent of certificate expiration) is the responsibility of the credential issuer (in particular, the certificate authority (CA) that provides the PIV authentication (PIV Auth) certificate). When an individual is no longer a valid credential holder, a revocation request is sent to the CA and that credential/certificate is placed on the certificate revocation list (CRL). A number of certificate validation techniques (on-line certificate status protocol [OCSP], server certificate validation protocol [SCVP] and identity and privilege list [IPL]) then leverage the signed CRL to provide certificate and identity status to the logical access, physical access and mobile credential validation applications.

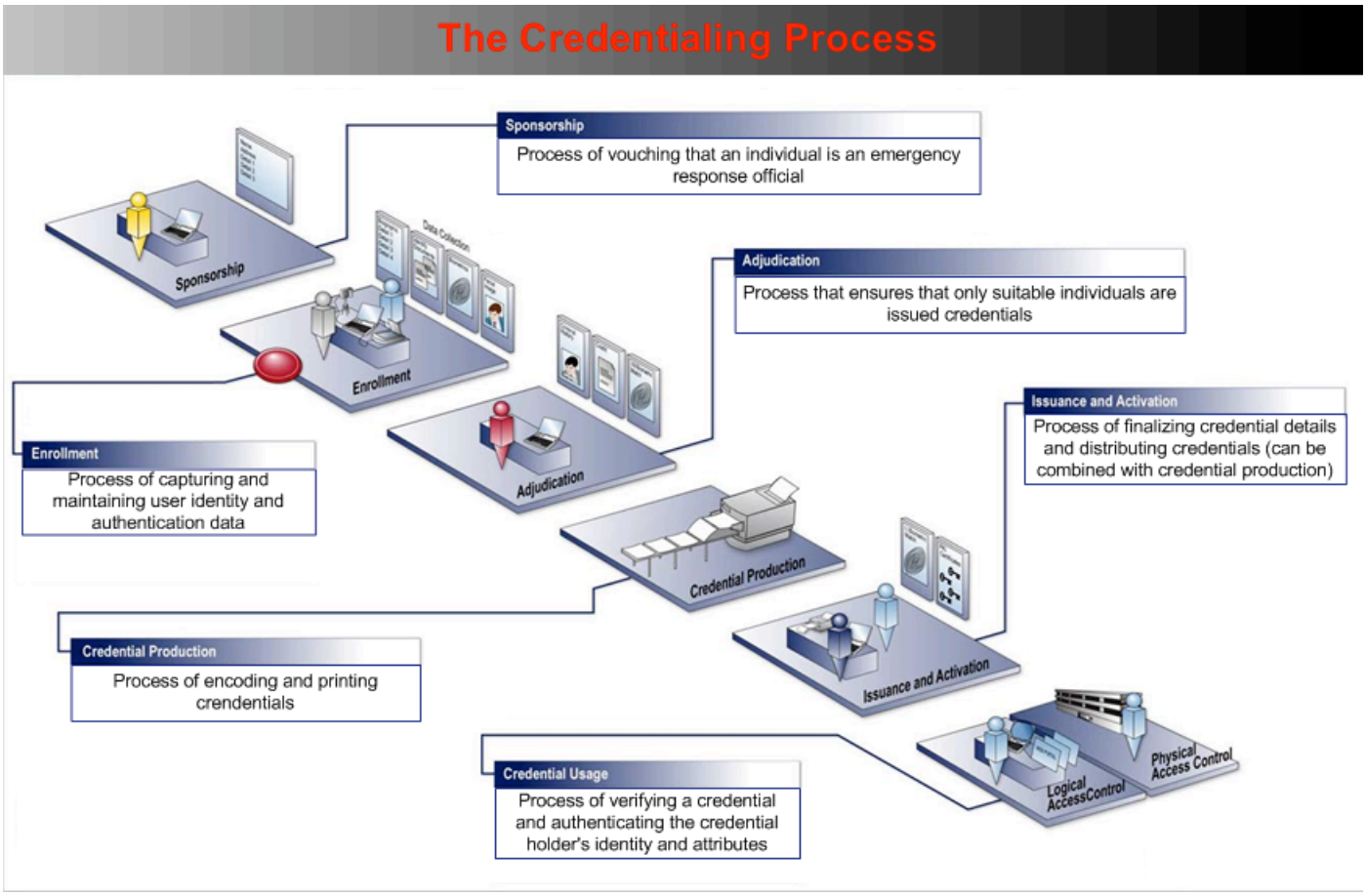


Figure 1: Example of ERO Credentialing Process

5 Conclusions

FIPS 201 provides a compelling architecture for identity assurance. A FIPS 201 credential provides strong authentication for access control, PKI-enabled applications, and other transactions. A FIPS-201 ERO credential is an interoperable credential that attains trust across multiple jurisdictions for disaster response and recovery. The population of EROs is growing and includes public and private sector personnel in the Federal, state, local, and tribal governments, volunteer organizations, and critical infrastructure organizations. Tens of millions of people working for a wide variety of public and private organizations are potential EROs.

All organizations in the emergency response community should take advantage of the experience of the Federal, state, and commercial organizations that are now deploying FIPS 201-interoperable credentials. Implementing a FIPS 201-based ERO credential leverages the Federal FIPS 201 and emergency response infrastructure investment along with commercial industry's investment in products that support this standard. Only an interoperable credential can fully leverage this experience and investment. Only a FIPS 201 smart card can meet the needs of first response and recovery and the requirements of chief information officers and corporate security directors who are looking for a cost-effective solution for secure physical and logical access. Continuity of operations needs are also best met with interoperable credentials that serve as the basis for identification and mutual aid.

This white paper identifies best practices and defines use cases for ERO credentials that meet the identity goals of trust, privacy, interoperability, and usability. DHS and many states are now demonstrating or piloting ERO credentialing programs. These programs use many of the processes and features that will be needed for large scale programs and are helping to define how ERO credentials will be implemented nationwide. Additional information on ERO credentialing standards and pilots is available from DHS/FEMA.[14]

The Smart Card Alliance encourages organizations that are involved in the important role of emergency response and recovery and that are now reviewing their identity, access, and credentialing requirements to consider a FIPS 201 smart card-based credential as the foundation for their credentialing programs.

[14] For additional information, the DHS/FEMA FRAC support team can be contacted at +1-202-646-2634.

6 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Identity Council and Physical Access Council to describe the benefits of using FIPS 201-based smart cards for ERO credentials and present credential use cases that support both emergency response and daily use. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank Identity and Physical Access Council members for their contributions, including: BearingPoint, CardLogix, Cogent Systems, CoreStreet, Diebold, EDS, Fargo Electronics, Gemalto, HID Global, Hirsch Electronics, IDmachines, IDTP, IQ Devices, Northrop Grumman, Oberthur, Probaris, Sagem Morpho, Thales e-Security, Tyco International, U.S. Department of Homeland Security, U.S. Department of State.

Special thanks go to Tony Cieri, Tom Lockwood, Debbie Sottile, and Craig Wilson from DHS/FEMA for their comments and contributions and to the following Identity and Physical Access Council members who participated in the white paper development:

- Consuelo Bangs, Sagem Morpho
- Ben Black, BearingPoint
- Kirk Brafford, Cogent Systems
- Kathleen Carroll, HID Global
- Nathan Cummings, HID Global
- Sal D'Agostino, IDmachines
- Tony Damalas, Diebold
- Walter Hamilton, IDTP
- Steve Howard, Thales e-Security
- Lolie Kull, EDS
- LaChelle LeVan, Probaris
- Gilles Lisimaque, IDTP
- Ola Martins, Oberthur
- John McGeachie, CoreStreet
- Cathy Medich, Smart Card Alliance
- Bob Merkert, CardLogix
- Neville Pattinson, Gemalto
- Dwayne Pfeiffer, Northrop Grumman
- Roger Roehr, Tyco International
- Steve Rogers, IQ Devices
- John Santisteban, Fargo Electronics
- Dan Schleifer, CoreStreet
- Mike Sulak, Department of State
- Lars Suneborn, Hirsch Electronics
- Mike Zercher, HID Global

The Smart Card Alliance would also like to thank CardLogix for the graphics in Section 2 and BearingPoint for the graphic in Section 4.

About the Smart Card Alliance Identity Council

The Smart Card Alliance Identity Council is focused on promoting the need for technologies and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud, and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.

About the Smart Card Alliance Physical Access Council

The Smart Card Alliance Physical Access Council is focused on accelerating the widespread acceptance, usage, and application of smart card technology for physical access control. The group brings together, in an open forum, leading users and technologists from both the public and private sectors and works on activities that are important to the physical access industry and that will address key issues that end user organizations have in deploying new physical access system technology. The Physical Access Council includes participants from across the smart card and physical access control system industry, including end users; smart card chip, card, software and reader vendors; physical access control systems vendors; and integration service providers.

Identity and Physical Access Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.

Additional information about the Identity and Physical Access Councils and about the use of smart cards for secure identity and access applications can be found at http://www.smartcardalliance.org.

7 Appendix A: ERO Credential Pilots

A number of recent demonstrations and pilots of ERO programs have implemented and tested different use cases for a FIPS 201-based ERO credentialing system, including programs that involved emergency response officials in the NCR, Virginia, Maryland, Pennsylvania, Texas, Illinois, Florida, and Colorado.

7.1 ERO Credential Demonstrations

"H.R. 1: Implementing Recommendations of the 9/11 Commission Act of 2007," was introduced into Congress on January 5, 2007 and signed into law by the President on August 3, 2007.[15] Under HR-1, the Federal Emergency Management Agency (FEMA) is responsible for issuing credentialing and attribute standards for first response across the nation. The first step is to establish federal preparedness, to be followed by outreach to state and local communities, the critical infrastructure communities, and the volunteer communities.

Since HR-1 was introduced, several demonstrations were held to test the credentialing and attributes of the various emergency response communities. These demonstrations were named Winter Storm[16,17] (February 2007), Summer Breeze (July 2007), Winter Blast[18,19] (March 2008), Spring Blitz[20] (May 2008), and Summer Sizzle (July 2008). A number of other demonstrations took place before HR-1 that involved additional scenarios.

At the Winter Storm demonstration, FIPS 201 ERO credentials were validated, and attributes (typically ESF code or NIPP sector) or roles were determined in a number of environments. Agencies were able to validate credentials and privileges for all FIPS 201-compatible and interoperable credentials, including the FRAC, TWIC, Mariner Administrative Card (MAC), and other legacy credentials such as the DoD CAC, which includes the National Guard population, and driver's licenses. These credentials were issued by a wide range of organizations, yet through adherence to standards, they were able to interoperate with a high level of trust and identity assurance. In the case where these credentials were not available, the demonstration was able to take other forms of identification (typically a driver's license) but without the same level of assurance.

The Summer Breeze disaster preparedness demonstration validated the capability of EROs from multiple jurisdictions to be rapidly authenticated, electronically, for both identity and the attributes (again ESF code and NIPP sector) as defined in the National Response Framework (NRF). The demonstration validated the ability to remove obstacles associated with *ad hoc* credentialing processes ("just-in-time credentialing"), including those experienced by emergency response officials supporting the Pentagon during the 9/11 terrorist attacks or the Hurricane Katrina aftermath.

The Summer Breeze FRAC usage demonstration was co-hosted by the DHS FEMA Office of National Capital Region Coordination (NCRC) and DoD Pentagon Force Protection Agency (PFPA). The demonstration highlighted federal, state, local, and private sector identity interoperability as well as the ability of FIPS 201-compatible and interoperable credentials to support applications beyond physical and logical access, including identification at any type of event or location.

The Winter Blast exercise was a far more extensive exercise than those that preceded it. As part of HR-1, FEMA is cooperating with the Department of Health and Human Services (HHS) for credentials and attributes of medical professionals. Four different scenarios were tested. They included the electronic validation of state emergency volunteers and mutual aid EROs, the ingress of Federal and mutual aid EROs, and assembly at a rally point for continuity of government egress to relocation sites.

[15] http://www.govtrack.us/congress/bill.xpd?bill=h110-1
[16] http://www.secureidnews.com/audio/iab_jan_07/winterstorm_iab_0107.pdf
[17] http://secureidnews.com/audio/iab_april_07/JonesandWilson.pdf
[18] http://www.secureidnews.com/audio/iab_0308/iab_0308_wilson.pdf
[19] http://www.secureidnews.com/audio/iab_0308/iab_0308_wilson.mp3
[20] http://www.secureidnews.com/news/2008/05/20/probaris-participates-in-spring-blast/

One of the main objectives was to ascertain that a robust credentialing process would be in place in an emergency situation in which communications were disrupted ("comms out"). The exercise achieved 100 percent validation of the credentials. In addition, Federal and non-Federal personnel collaborated completely in a trusted and distributed medical environment and on-scene medical surge assets were completely validated and accounted for electronically.

The recent Spring Blitz demonstration involved the City of Tampa and the National Football League to look at ERO scenarios around large-scale events—in particular, hurricane preparedness and the Super Bowl, which will be held in Tampa in early 2009.

The Summer Sizzle demonstration included the performance measures of all previous demonstrations but added HHS/FEMA-approved subcategory attributes. The ERO's identity and attributes were electronically validated and appeared on the mobile credential reader. The added benefit of knowing whether a physician is a thoracic surgeon or pathologist enables the incident scene commander to use assets more efficiently and effectively. The demonstration had three main objectives

1. FIPS 201 electronic validation of ESF 8, "Public Health and Medical Services," mutual aid EROs to include HHS/FEMA-approved subcategory skill sets
2. FIPS 201 electronic validation of Federal/state/local mutual aid EROs
3. FIPS 201 electronic validation of critical infrastructure/key resources (CI/KR) mutual aid EROs.

All performance measures were completely met during this demonstration.

Future plans include populating the Federal Emergency Response Official Attribute Repository within the NCR; working with NCR stakeholders to develop business rules and deployment model for national implementation; working with the Emergency Management Assistance Compact (EMAC) for interstate mutual aid credentialing and typing integration; working with Federal and non-Federal stakeholders to integrate usage into daily functionality for physical and network access permissions; working with private sector practitioner communities for critical infrastructure implementation and integration; and working with volunteer practitioner communities for proactive implementation and integration.

7.2 Commonwealth of Virginia First Responder Authentication Credentials

EROs from across the region were present at the Pentagon site on 9/11, including EROs from Arlington County and the City of Alexandria. Immediately following the attacks, onlookers were able to mingle with rescuers. This presented a serious challenge for incident commanders—to make sure that only credentialed EROs had access to the most sensitive areas. It became evident that a credentialing process was needed to simplify this effort in the future.

In February 2007, as part of the DHS (NCR) First Responder Partnership Initiative, the Virginia Department of Transportation and Commonwealth of Virginia began issuing FRACs. The Virginia FRAC identity proofing and registration processes follow FIPS 201 as closely as possible for a non-Federal entity and use products from the FIPS 201 GSA APL. The design of the Virginia FRAC card is also based upon FIPS 201.

The goal of the FRAC initiative, now being piloted in the NCR and Hampton Roads area, is to provide state and local EROs with a new, Federally-approved smart credential designed to achieve the following:

- Securely establish emergency responders' identities at the scene of an incident
- Confirm first responders' qualifications and expertise, allowing incident commanders to dispatch them quickly and appropriately

- Enhance cooperation and efficiency between state and local first responders and their federal counterparts[21]

Using a wireless handheld device, commanders at an incident scene can read data from the FRAC and authenticate the ERO's identity and attributes.

Among the first localities in Virginia to be issued the new FRACs were Arlington County and the City of Alexandria. Virginia has currently issued over 2,300 FRACs, which have been used in many of the nation's first tests of these new, state-of-the-art ERO identity credentials.

7.3 Colorado First Responder Authentication Credential

Colorado identified as a high priority the need for an interoperable first responder credential. The Colorado first responder authentication credential (COFRAC) initiative provides the ability to electronically validate the identity and the attributes (qualifications, certifications, authorizations, and privileges) of those who are required – or volunteer – to respond to natural or man-made disasters or acts of terror.

In June 2007, a Statewide Credentialing Working Group was formed, chaired by Governor's Office of Information Technology (OIT). This Working Group, comprised of individuals at the State, Regional and Local levels, has developed a program that addresses the needs of Colorado, while being mindful of the Federal standards and the need for interoperability with Federal agency responders. The overall goal of this working group was to provide recommendations for a common identification standard for State and Local first responders that promotes interoperable first responder credentials across the State and:

- Primarily, to achieve appropriate security assurance by efficiently verifying the claimed identity of individuals seeking physical access to all-hazard incidents and events in the State of Colorado.
- Secondarily, to communicate the qualifications, skills and training of first responder personnel to the Receiving Authority Incident Command.
- Finally, to base the program upon recognized standards, open-system architectures, and non-proprietary technologies.

The COFRAC standard is focused on incident management and interoperability, and does not specify access control policies or requirements for State departments and local agencies. State and local departments and agencies were encouraged, however, to investigate how the FRAC technology can be leveraged for both physical and logical access.

The Colorado credentialing standard was published in April 2008.[22]

Colorado's North Central Region (metropolitan Denver area) will begin its COFRAC pilot in October 2008, and should be issuing credentials that comply with the COFRAC standard by the first quarter of 2009 (calendar year).

[21] http://www.govtech.com/gt/articles/104398

[22] *Colorado State First Responder Authentication Credential Standards: Best Practice Standard*, Colorado Governor's Office of Information Technology, April 10, 2008 (available at https://publish.colorado.gov/cs/Satellite/OIT-New/OITX/1200536168031?rendermode=preview-lplunkett-1165692952165)

8 Appendix B: Emergency Support Function Codes and National Infrastructure Protection Plan Sectors

8.1 Emergency Support Function Codes

The following are the currently defined Emergency Support Function (ESF) codes:

1. Transportation
2. Communications
3. Public Works and Engineering
4. Firefighting
5. Emergency Management
6. Mass Care, Emergency Assistance, Housing and Human Services
7. Logistics Management and Resource Support
8. Public Health and Medical Services
9. Search and Rescue
10. Oil and Hazardous Materials Response
11. Agriculture and Natural Resources
12. Energy
13. Public Safety and Security
14. Long Term Community Recovery
15. External Affairs

8.2 National Infrastructure Protection Plan Sectors

The following are the currently defined National Infrastructure Protection Plan (NIPP) sectors:

1. Agriculture and Food
2. Banking and Finance
3. Chemical
4. Commercial Facilities
5. Dams
6. Defense Industrial Base
7. Emergency Services
8. Energy
9. Government Facilities
10. Information Technology
11. National Monuments and Icons
12. Commercial Nuclear Reactors, Materials and Waste
13. Postal and Shipping
14. Public Health and Healthcare
15. Telecommunications
16. Transportation Systems
17. Drinking Water and Water Treatment Systems
18. Critical Manufacturing

9 Appendix C: Glossary

Attribute
A qualification, certification, or skill set associated with a credential holder.

Authentication:
The process of electronically validating the identity and/or attribute of a person or other entity.

CAC (Common Access Card)
The identification card issued by the Department of Defense to all employees and contractors.

Digital certificate
Digital documents (e.g., information such as the name of the person or an organization and their address) attesting to the binding of a public key to an individual or other entity. Digital certificates allow verification of the claim that a specific public key does in fact belong to a specific individual.

Emergency Support Function
See ESF.

ESF (Emergency Support Function)
Primary mechanism at the operational level used to organize and provide assistance. Defined by FEMA as part of the National Response Framework (NRF).

FIPS 201
Federal Information Processing Standard 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*.

FIPS 201-compliant
Term describing an entity that meets all of the requirements of the FIPS 201 standards. By definition, only Federal agencies from the Executive Branch of the government to which HSPD-12 applies can issue FIPS 201-compliant credentials.

First Responder Authentication Credential
See FRAC.

FRAC (First Responder Authentication Credential)
A smart card-based credential that provides first responders from across the National Capital Region with the ability to quickly and easily access government buildings and reservations in the event of a terrorist attack or other disaster. The FRAC is part of the Office of National Capital Region Coordination's initiative to develop a smart identity card system for emergency responders.

Flash pass
An ID card that is shown (or flashed) to a person who visually verifies that the cardholder is the person who owns the card.

Identity
The subset of physical and/or behavioral characteristics by which an individual is uniquely recognizable. Identity is information concerning the person, not the actual person.

Logical access
Access to online resources (e.g., networks, files, computers, databases).

National Infrastructure Protection Plan
See NIPP.

NIPP (National Infrastructure Protection Plan)
A coordinated approach to critical infrastructure and key resources (CIKR) protection roles and responsibilities for federal, state, local, tribal, and private sector security partners. Defined by DHS, the NIPP sets national priorities, goals, and requirements for effective distribution of funding and resources which will help ensure that our government, economy, and public services continue in the event of a terrorist attack or other disaster.

PACS (Physical access control system)
A system composed of hardware and software components that control access to physical facilities (e.g., buildings, rooms, airports, warehouses).

Personal identity verification card
See PIV card.

Physical access control system
See PACS.

PIV card (**Personal identity verification card**)
The dual-interface smart card that is being issued to all Executive Branch Federal employees and contractors and that will be used for both physical and logical access.

PIV-compatible card
A card that meets the FIPS 201 technical specifications. PIV infrastructure elements such as card readers are capable of working with such cards, but the credential itself has not been issued in a way that assures it is trustworthy by Federal relying parties.

PIV-interoperable card
A card that meets the FIPS 201 technical standards and is issued in a way that allows Federal relying parties to trust the credentials.

PKI (Public key infrastructure)
The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. There are four basic components to the PKI: a certificate authority, who is responsible for issuing and verifying digital certificates, a registration authority, which provides verification to the certificate authority before issuing digital certificates, one or multiple directories to hold certificates (with public keys), and a system for managing the certificates. Also included in PKI are the certificate policies and agreements among parties that document the operating rules, procedural policies, and liabilities of the parties operating within the PKI.

Privilege
Authorization or access granted to credential holders based on the authentication of their identity and attributes.

Public key infrastructure
See PKI.

Transportation Worker Identification Credential
See TWIC.

TWIC (Transportation Worker Identification Credential)
A common smart card-based identification credential for all personnel requiring unescorted access to secure areas of Maritime Transportation Security Act-regulated facilities and vessels, and all mariners holding Coast Guard-issued credentials.