Why are credentialing and interoperability important?

Credentialing proves two things:

- A person is who they claim they are; and
- A person is still serving in the role under which the credential was issued.

At an event, credentials can be used to register attendees, track where they go, and prove when they leave. Credentials also can track assets and ensure that roles and responsibilities are being followed. Thanks to a standard for interoperability, a single credential can replace two or more proprietary credentials across multiple access control measures.

How do I know my identity card is interoperable?

When credentials are issued in accordance with the FIPS 201 standard, they may be trusted by other credential issuers and are technically interoperable. The only interoperable identity cards accepted at OMB Assurance Level (AL) 4 for authentication are PIV, PIV-I, CAC, and a PIV-I-compliant FRAC. By the standard definition, these identity cards meet the NIST technical specifications to work with the PIV infrastructure elements, such as card readers, and are issued in a manner that allows federal government relying parties to trust the card. These identity cards also allow local, state, federal, and private partners to be interoperable and trusted across multiple jurisdictions. Although the cards are interoperable, access privileges are always determined by the facility or network administrator and system owner.

Is there current guidance for credentialing emergency response personnel?

The National Incident Management System (NIMS) Guideline for the Credentialing of Personnel issued by the Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA) strongly encourages state, local, tribal jurisdictions as well as the public and private sector entities to leverage the federal investment in the FIPS-201 infrastructure. The document also endorses the Federal Chief Information Officer's PIV-I guidance to promote trust, facilitate interoperability for personnel deployed outside their home jurisdiction, and the ability to make informed decisions for access permissions. Additionally, HSPD-5 requires federal departments and agencies to make adoption of NIMS by state, local, and tribal governments a condition for federal preparedness assistance through grants, contracts, and other activities.

DOCUMENTS AND REFERENCES

HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors
Sets a standard for secure and reliable forms of identification
http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors
http://csrc.nist.gov/publications/PubsFIPS.html

Personal Identity Verification Interoperable (PIV-I) Frequently Asked Questions (FAQ)
http://www.idmanagement.gov/documents/PIV-I_FAQ.pdf

Moving Toward Credentialing Interoperability (DHS S&T Case Study Document)
http://www.cyber.st.dhs.gov

Department of Defense Acceptance of PIV-I
http://www.doncio.navy.mil/Download.aspx?AttachID=1375

NIMS Guideline for the Credentialing of Personnel
http://www.fema.gov/pdf/emergency/nims/nims_cred_guidelines_report.pdf

OMB Memorandum 11-11: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 — Policy for a Common Identification Standard for Federal Employees and Contractors
http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf

FOR ADDITIONAL INFORMATION

http://www.ahcusa.org/PIV-I%20TTWG.htm
TTWGinformation@hq.dhs.gov

Who Is This Person and Do I Let Them In?

Achieving Credentialing Interoperability — A Proven and Scalable Solution

PIV-I/FRAC Technology Transition Working Group

Homeland Security
Science and Technology

BACKGROUND

Local, state, federal, and private-sector agencies are working to establish an interoperable credential called the Personal Identity Verification-Interoperable (PIV-I) card in their own organizations and jurisdictions. Toward this end, federal agencies are rapidly deploying the Personal Identity Verification (PIV) card based on Homeland Security Presidential Directive (HSPD) 12. Providing a PIV or PIV-I card credential[1] provides a secure common identification. Emergency response officials are moving toward achieving credentialing interoperability by issuing a First Responder Authentication Credential (FRAC) that complies with the PIV-I standard specifications. However, for this to happen, many credentialing and badging challenges must be overcome.

In the past, the granting of physical access to sites would be based on personal judgment, flash pass using badges, and low-level electronic credentials rather than on hard, high-assurance identity verification. Logical access to computer systems required only a username and password. Today, Office of Management and Budget guidance (OMB 11-11) specifies that access to all federal facilities and computer systems requires secure forms of identification based on smart card technology and identity-proofing procedures.

Federal guidance on personnel credentialing can serve as a common blueprint that local, state, regional, federal, and private credentialing authorities can use to implement an interoperable credentialing system in their area. The PIV-I guidance provides the technical specifications that meet the PIV requirements as defined by Federal Information Processing Standard (FIPS) 201. An identity credential that meets these guidelines will be interoperable with, and trusted by, the Federal Government and any partnering jurisdictions.

The PIV-I guide for Non-Federal Issuers (NFIs)[2] provides organizations with a standard way to issue and accept a standard credential. In this way, emergency responders can respond to an incident using a trusted and interoperable credential or accept a credential issued in the same manner as their own. In turn, this standard eases both the financial and procedural burden of establishing bilateral trust mechanisms between jurisdictions.

PARTNERSHIPS

The Cyber Security Division (CSD) within the Department of Homeland Security's Science and Technology Directorate (S&T), the FEMA Office of the National Capital Region Coordination (NCRC), the FEMA office of the Chief Security Officer (OCSO), and the FEMA Office of the Chief Information Officer (OCIO) have partnered to form the PIV-I/FRAC Technology Transition Working Group (TTWG). The TTWG is composed of federal, state, and local emergency management representatives, many of whom have already implemented innovative and secure identity-management solutions in their own jurisdictions.

The working group serves several purposes:

- Share information and lessons learned: state-to-state, state-to-federal, federal-to-state.
- Provide federal policy makers a unified state-level emergency-manager perspective on Federal/Emergency Response Official (F/ERO) attributes.
- Baseline current identity infrastructures and best practices to share with stakeholders.
- Identify technological gaps where CSD can support research and development.

EMERGENCY RESPONSE SPECTRUM

Access to all federal buildings and computer systems will require secure forms of identification based on smart card technology and trusted identity-proving procedures. Smart cards replace pre-existing federal credentials and enable an electronic verification capability that can confirm whether a presenter's identity and access privileges are valid and current.

For physical access, a building guard will use an electronic reader to access information on the card and check it against a database to confirm a person's identity and verify that the person has the proper clearance to enter the building. For logical access, hardware will scan the same card to determine whether the person is allowed to access a government network, and, ideally, what files and applications the holder can view.

While local, state, regional, federal, and private credential issuers may choose to issue other types of credentials, PIV-I is the only credentialing standard accepted by the Federal Government to ensure interoperability and a high level of trust. With PVI-I support and the collaboration of partners from different levels of government, our nation can ensure more secure and cost effective identity/attribute management and credentialing practices.

FREQUENTLY ASKED QUESTIONS

What is an identity credential?

According to FIPS 201, a credential is "evidence attesting to one's right to credit or authority." A credential is issued to an individual by an authoritative source, which binds the individual's identity to the credential that the individual possesses and controls. The identity credentials issued can range from a username and password to a smart card. The standards for PIV and PIV-I specify the implementation of a person's identity credentials onto an identity card with an integrated circuit chip (*for example, a smart card*). These identity cards may be used on PIV-compliant authentication systems. Additional credentials and attributes about the person, such as training and certifications, will need to be validated through an attribute exchange mechanism.

What are PIV, PIV-I, CAC, and FRAC cards?

PIV, PIV-I, CAC, and PIV-I-compliant FRAC are interoperable smart card credentials. The acronyms stand for:

- **PIV** – Personal Identity Verification (*credential for federal employees*)
- **PIV-I** – Personal Identity Verification Interoperable (*credential for nonfederal employees*)
- **CAC** – Common Access Card (*PIV credential for Department of Defense employees*)
- **FRAC** – First Responder Authentication Credential (PIV-I *credential for emergency responders*)

PIV, PIV-I, and CAC are the only interoperable smart card identification credentials that fully conform to FIPS 201 and National Institute of Science and Technology (NIST)-related standards and meet their technical specifications. Please note that FIPS 201 is for federal entities; Non-Federal Issuers must follow the PIV-I for NFI guide issued by the Federal CIO Council. Only FRAC-issued cards that adhere to this guide are interoperable.

1 *Law enforcement officials often refer to their credentials as badges; therefore, from this point forward, this document will often use "credentials" to mean "badges" for the law enforcement community.*

2 Personal Identity Verification Interoperability For Non-Federal Issuers, http://www.cio.gov/Documents/PIV_Interoperabillity_Non-Federal_Issuers_May-2009.pdf