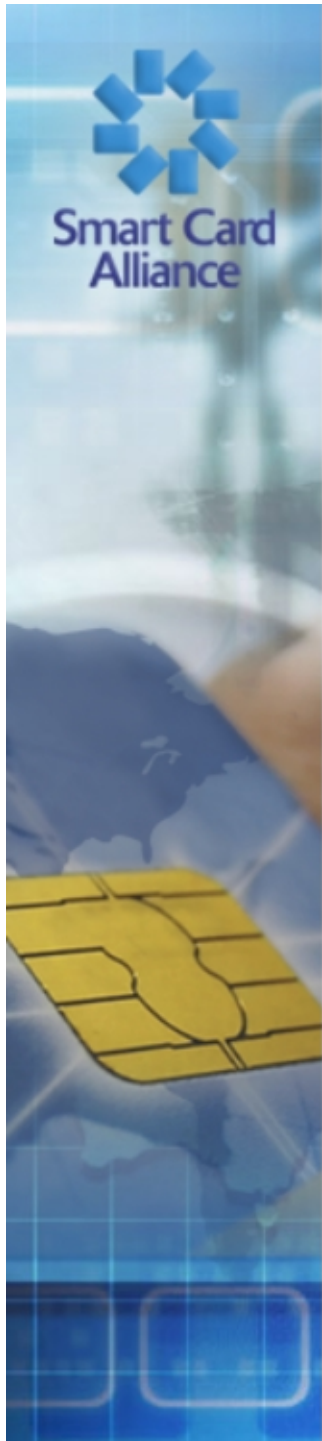# Emergency Response Official Credentials A Smart Card Alliance White Paper

Salvatore D'Agostino

CEO, IDmachines LLC

sal@idmachines.com

Smart Card Alliance

- **Broad collection of professionals working with all kinds of smart card technology. Members from public and private sectors**
- **Made up of industry councils**
  - ➢ Identity
  - ➢ Physical Access
  - ➢ Contactless and Mobile Payments
  - ➢ Transportation
  - ➢ Healthcare
- **Industry events and educational programs**
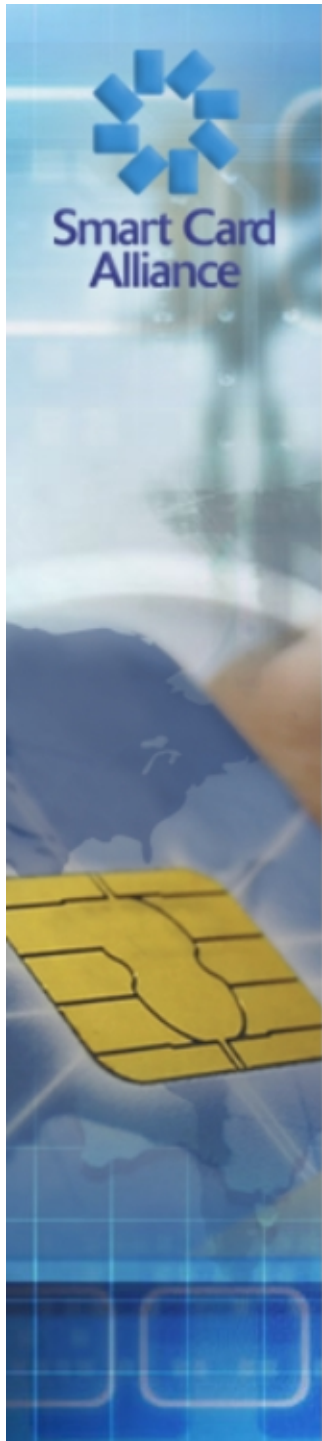- **www.smartcardalliance.org**
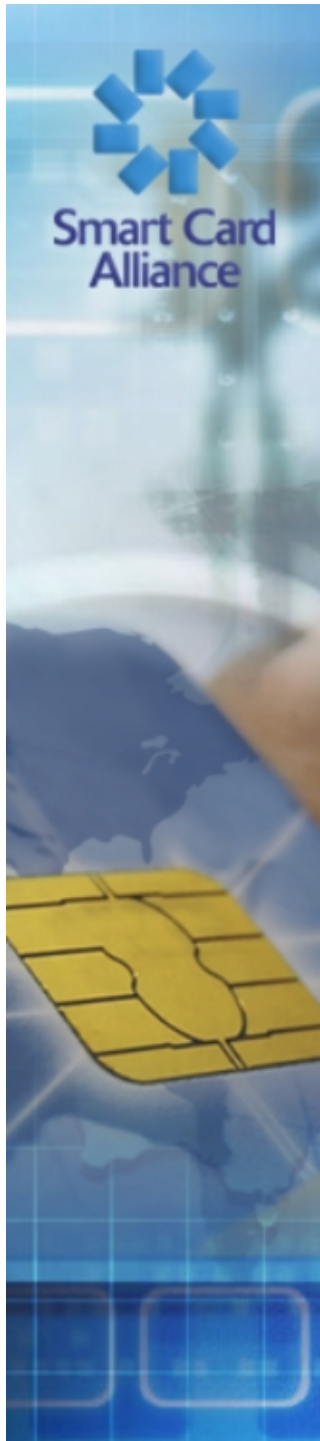
Identity and Physical Access Council Effort

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
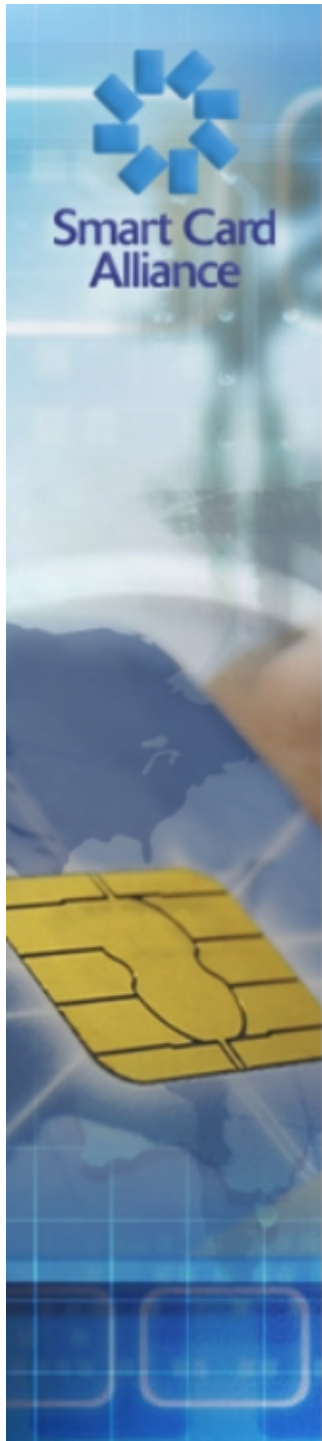Gilles Lisimaque, IDTP
Ola Martins, Oberthur

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

Tony Cieri, consultant, Tom Lockwood, Deb Sottile, Craig Wilson, Department of Homeland Security

Standard Strong Identity

- **Smart Card Alliance presents a strong recommendation to follow a FIPS 201 model**

- **Leverage commercially available products**

- **Leverage US Government investment**

- **Flexible adaptable platform**

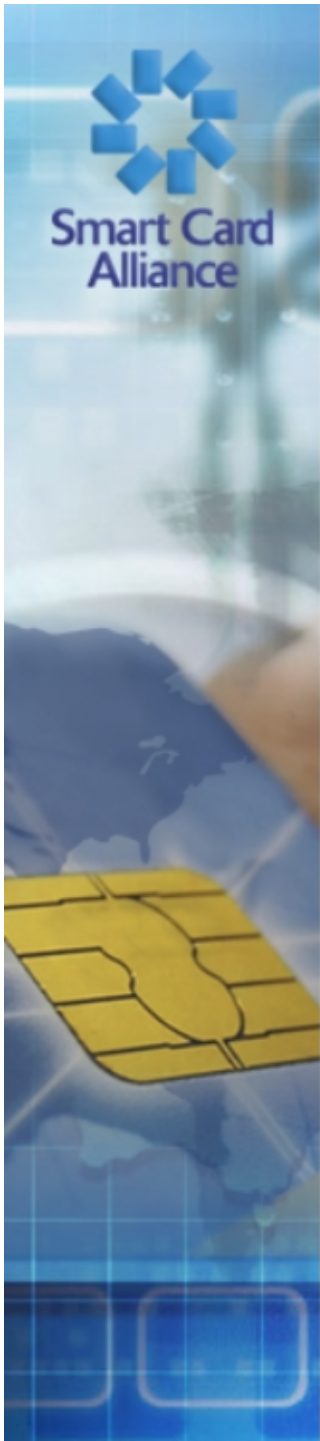- **Driven by high assurance, high availability and interoperability**

Identity as a Utility

- **Something you use every day**
  - ➢ Widely available
  - ➢ Easy to use
  - ➢ Safe

- **Same as electricity, roads or plumbing**

- **FIPS 201 is a multi-billion dollar identity infrastructure investment**

- **Smart credentials enable a wide range of applications that leverage this infrastructure and related products**
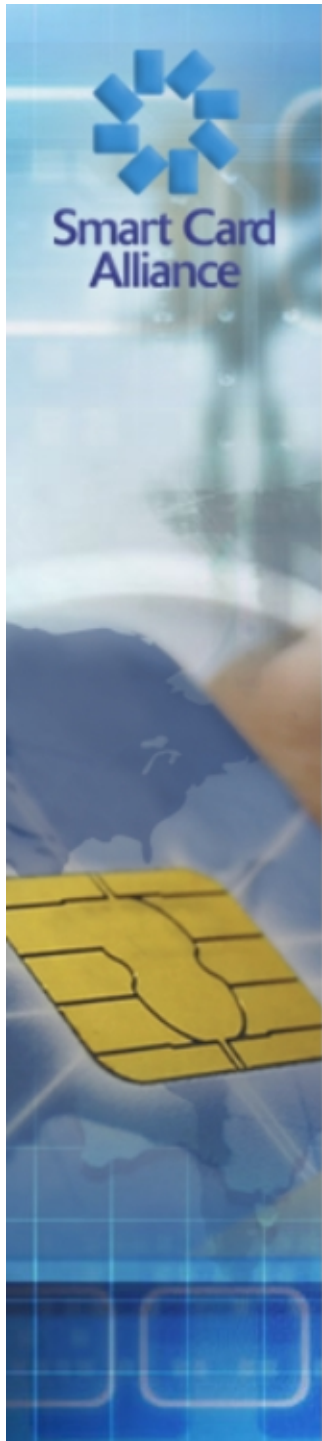
What is being put in place?

- **Federal Infrastructure to Support Identity and Typing**
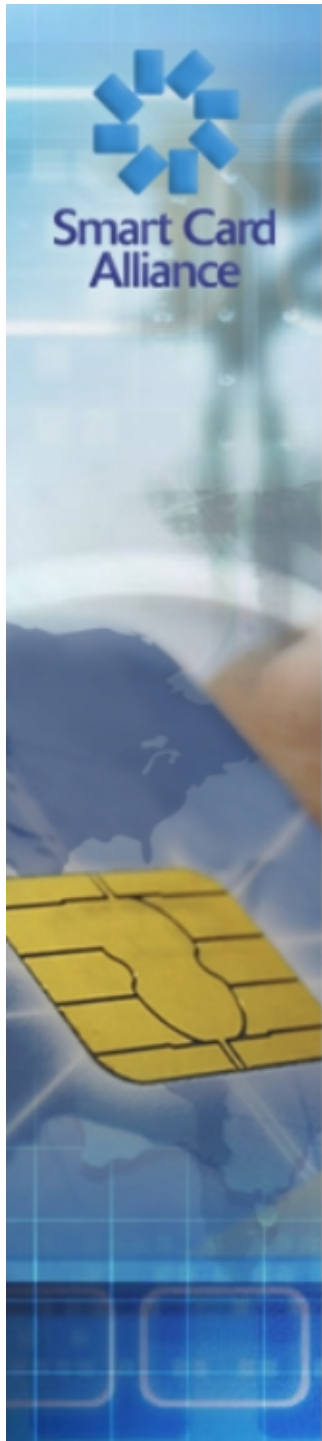- **Process for Establishing Trust of Identity and Typing**
- **Funding for Programs Choosing to Issue FIPS-201 Credentials (e.g. UASI funding in National Capitol Region)**
- **On-going demonstrations to expand community of interest and demonstrate applications**
- **Production ready, highly available and scalable**
- **Response to HR 1 (post 9-11 recommendations), Katrina**
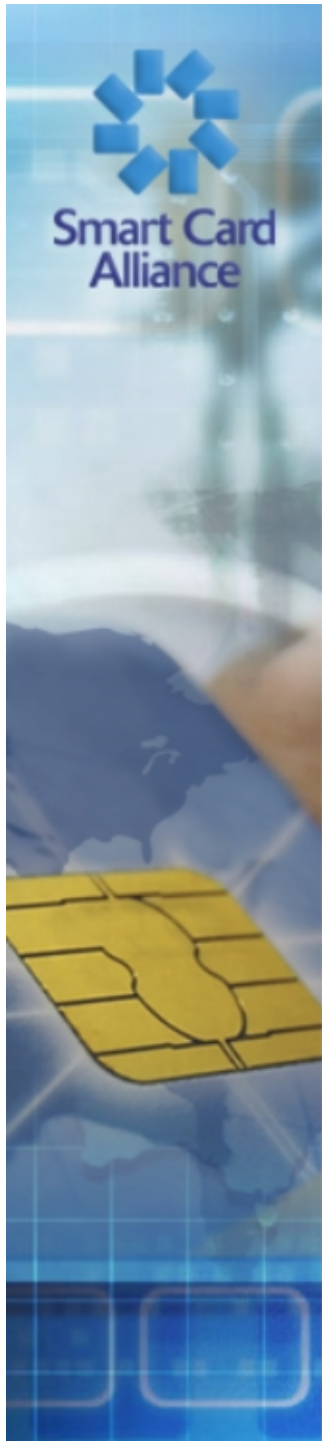
Identity and Privilege Infrastrucure

Smart Card Alliance

State and Local DMV

State and Local HR Databases

State and Local First Responder Databases

DoD

FEMA

Other State FRAC CAs (by agreement)

Other FBCA CAs

Federal, State and Local Identities and Privileges

Federal Bridge Certificate Authority (FBCA)

Shared Service Hosting

Privilege/Attribute

Licensures, Training Certifications, Downloaded From Enterprise

Privilege Management

1st responder CAs

Optional Local Hosting

Privilege/Attribute

Licensures, Training Certifications, Locally Administered

Identity

Synchronization Logs

Field Stations

Incident Scene Access

FIPS 201 and Flash Pass Credential Generation and Issuance

Photo, Fingerprint and Identity Validation

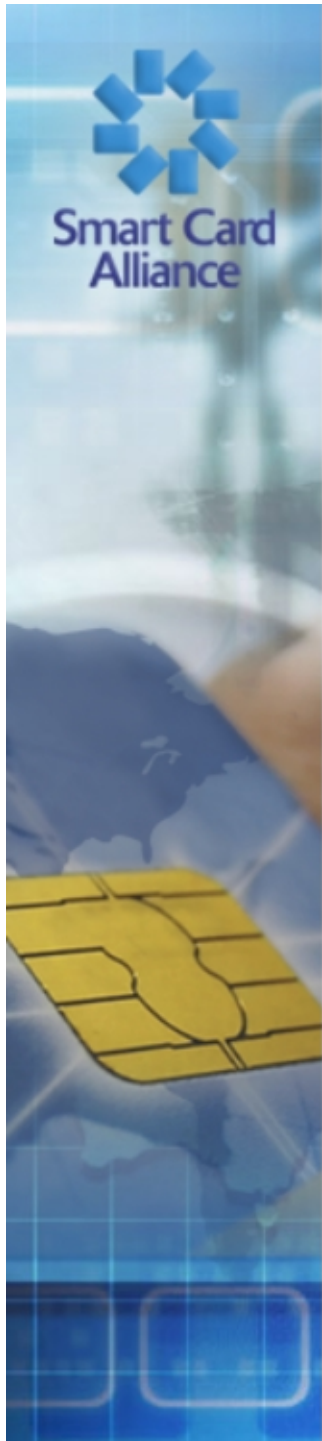= PKI authenticated and encrypted data transfers

Two Questions??

- **Who are you?**
  - ➤ Authentication
  - ➤ Trusted
  - ➤ Multiple factors
- **What are you allowed to do?**
  - ➤ Attributes
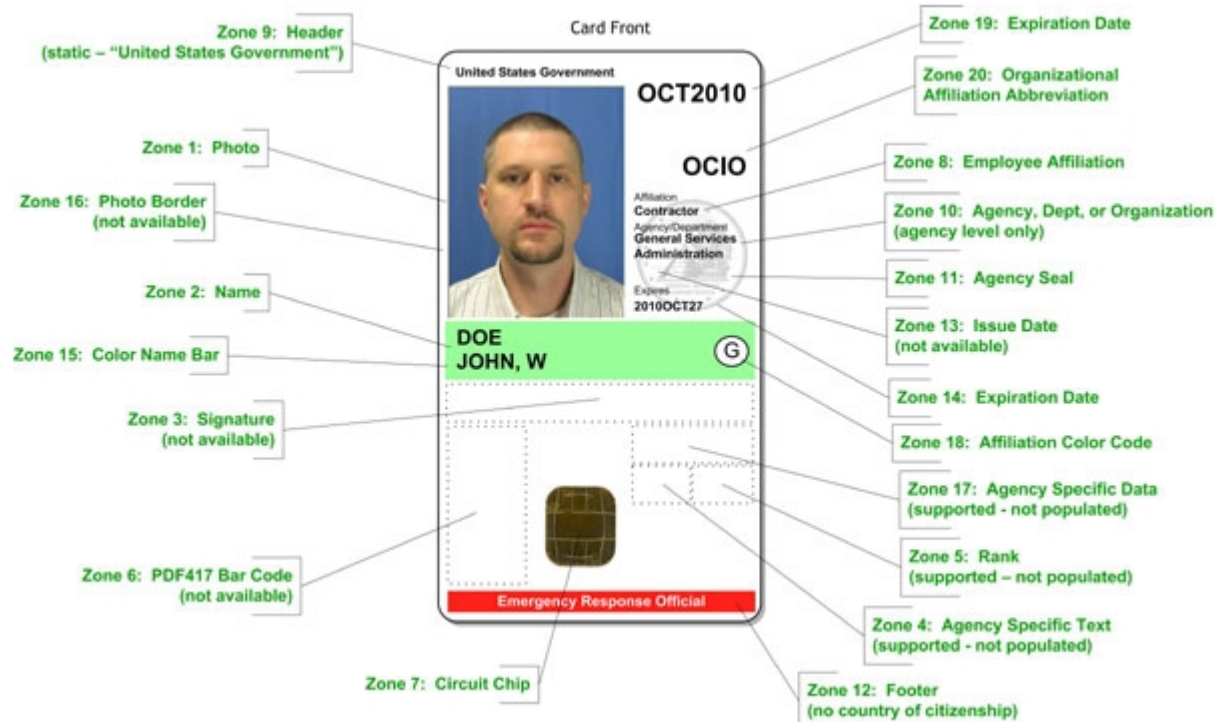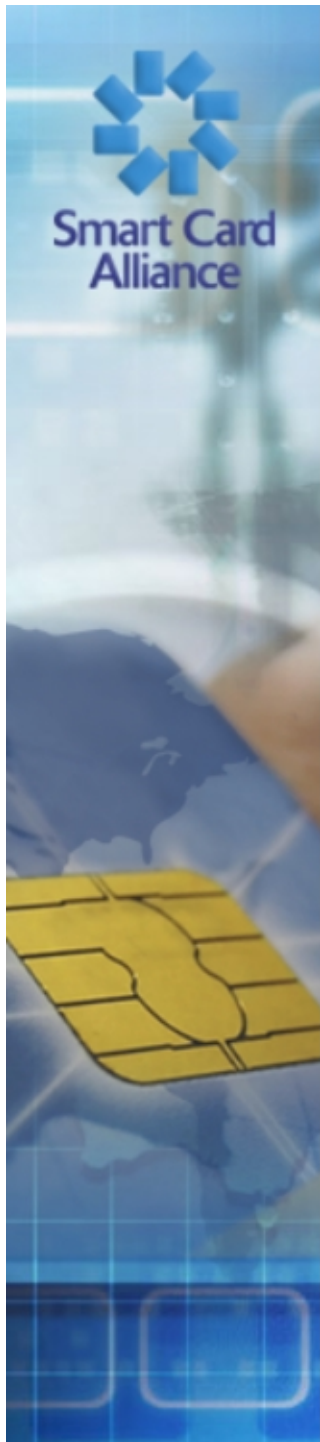 - ➤ Privileges/Authorization
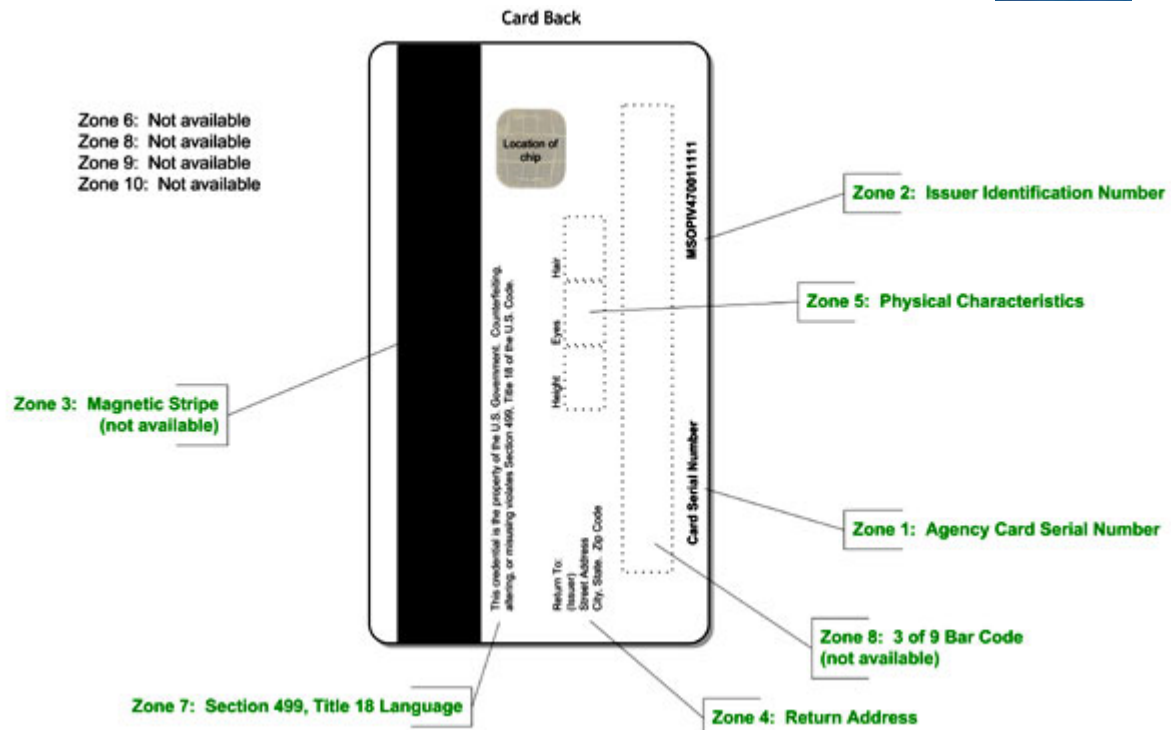
What is a FIPS 201 credential?

- **Integrated circuit chip (ICC):**
  - ➢ Four PKI digital certificates (PIV authentication, card authentication, digital signature and encryption)
  - ➢ Two interoperable fingerprint templates
  - ➢ Signed digital photo
  - ➢ Contactless interface
    - ➢ Physical Access, Payments, Optional Biometrics
  - ➢ Basis for strong assurance and interoperability

- **Other aspects:**
  - ➢ Cardholder Unique Identifier (CHUID) including organization affiliation, agency affiliation, department affiliation, and expiration date.
  - ➢ Optional Bar Codes to store key personal or other information (available in future releases), including:
  - ➢ Magnetic Stripe

What is a FIPS 201 credential?

- **Compliant**
  - ➤ Federal employees and their contractors
- **Interoperable**
  - ➤ Certificates are cross-certified to the Federal Bridge Certificate Authority
  - ➤ Assurance level agreed by policy a priori
  - ➤ Follows the standard for activation and lifecycle management of the credential
- **Compatible**
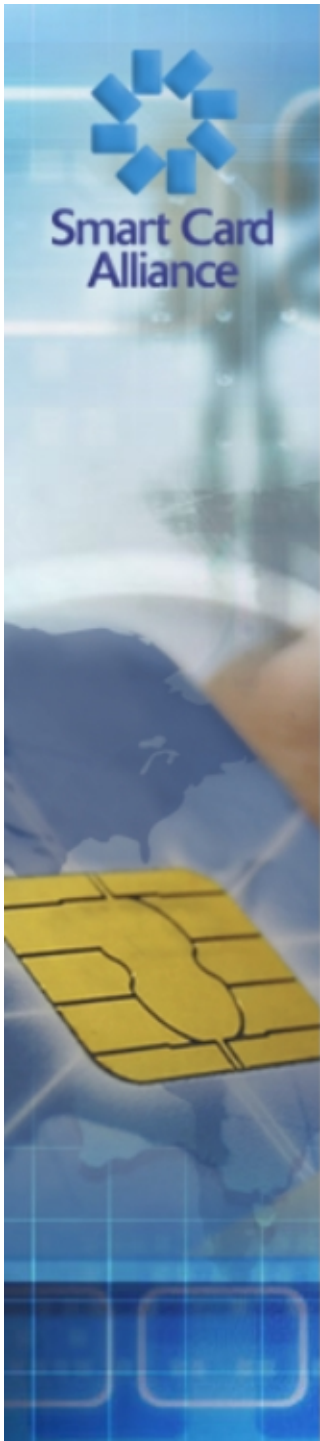 - ➤ Follows the technical standards FIPS 201 in the production of the credential

Smart Card Alliance

Smart Card Alliance

Card Front

Zone 9: Header
(static – "United States Government")

Zone 1: Photo

Zone 16: Photo Border
(not available)

Zone 2: Name

Zone 15: Color Name Bar

Zone 3: Signature
(not available)

Zone 6: PDF417 Bar Code
(not available)

Zone 7: Circuit Chip

Zone 19: Expiration Date

Zone 20: Organizational
Affiliation Abbreviation

Zone 8: Employee Affiliation

Zone 10: Agency, Dept, or Organization
(agency level only)

Zone 11: Agency Seal

Zone 13: Issue Date
(not available)

Zone 14: Expiration Date

Zone 18: Affiliation Color Code

Zone 17: Agency Specific Data
(supported - not populated)

Zone 5: Rank
(supported – not populated)

Zone 4: Agency Specific Text
(supported - not populated)

Zone 12: Footer
(no country of citizenship)

United States Government
OCT2010
OCIO
Affiliation
Contractor
Agency/Department
**General Services
Administration**
Expires
2010OCT27
DOE
JOHN, W
G
Emergency Response Official

Card Back

Zone 6: Not available
Zone 8: Not available
Zone 9: Not available
Zone 10: Not available

Location of chip

MSOPIV470011111

Zone 2: Issuer Identification Number

Zone 5: Physical Characteristics

Hair

Eyes

Height

Zone 3: Magnetic Stripe (not available)

This credential is the property of the U.S. Government. Counterfeiting, altering, or misusing violates Section 499, Title 18 of the U.S. Code.

Return To: (Issuer) Street Address City, State, Zip Code

Card Serial Number

Zone 1: Agency Card Serial Number

Zone 8: 3 of 9 Bar Code (not available)

Zone 7: Section 499, Title 18 Language

Zone 4: Return Address

Credentialing Process

Sponsorship

Enrollment

Adjudication

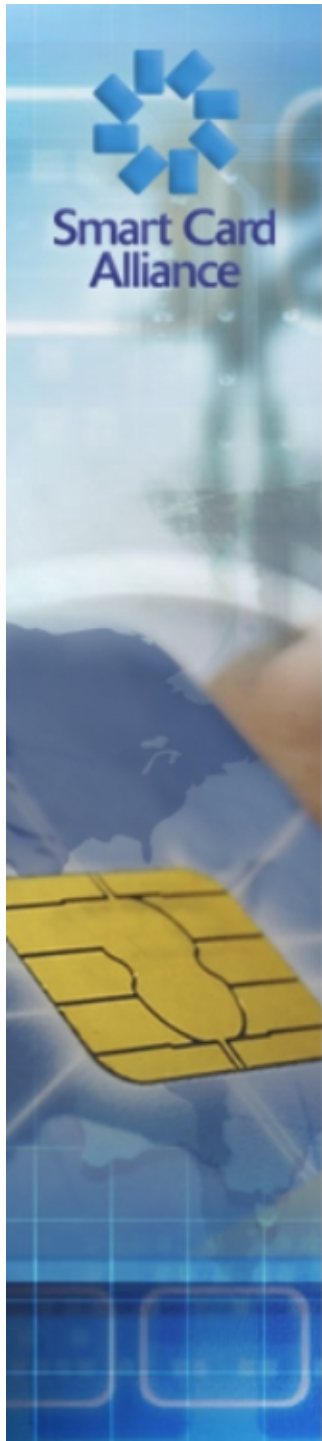**Credential Production**

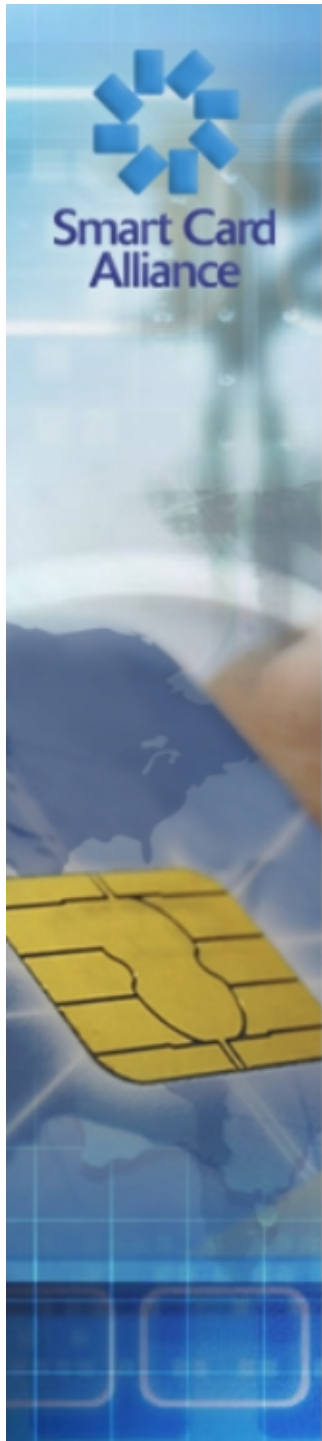**Issuance and Activation**

Use
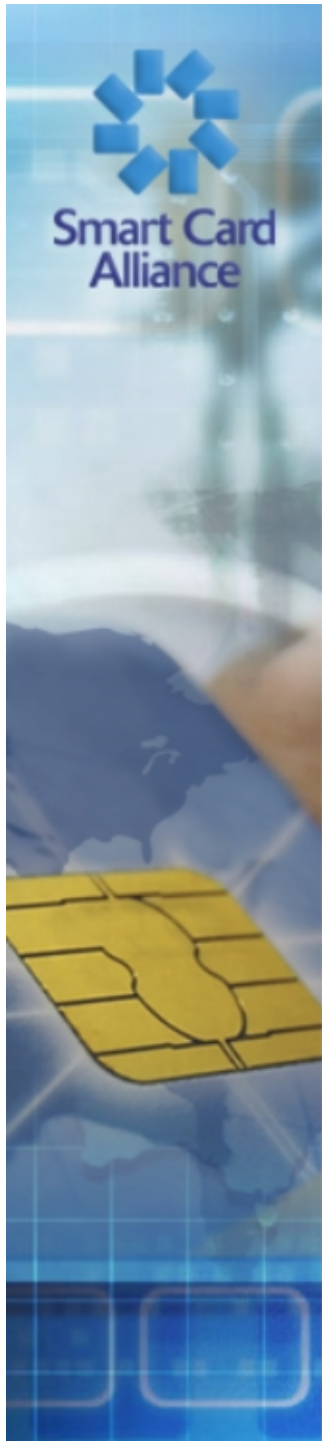
Credentialing Process
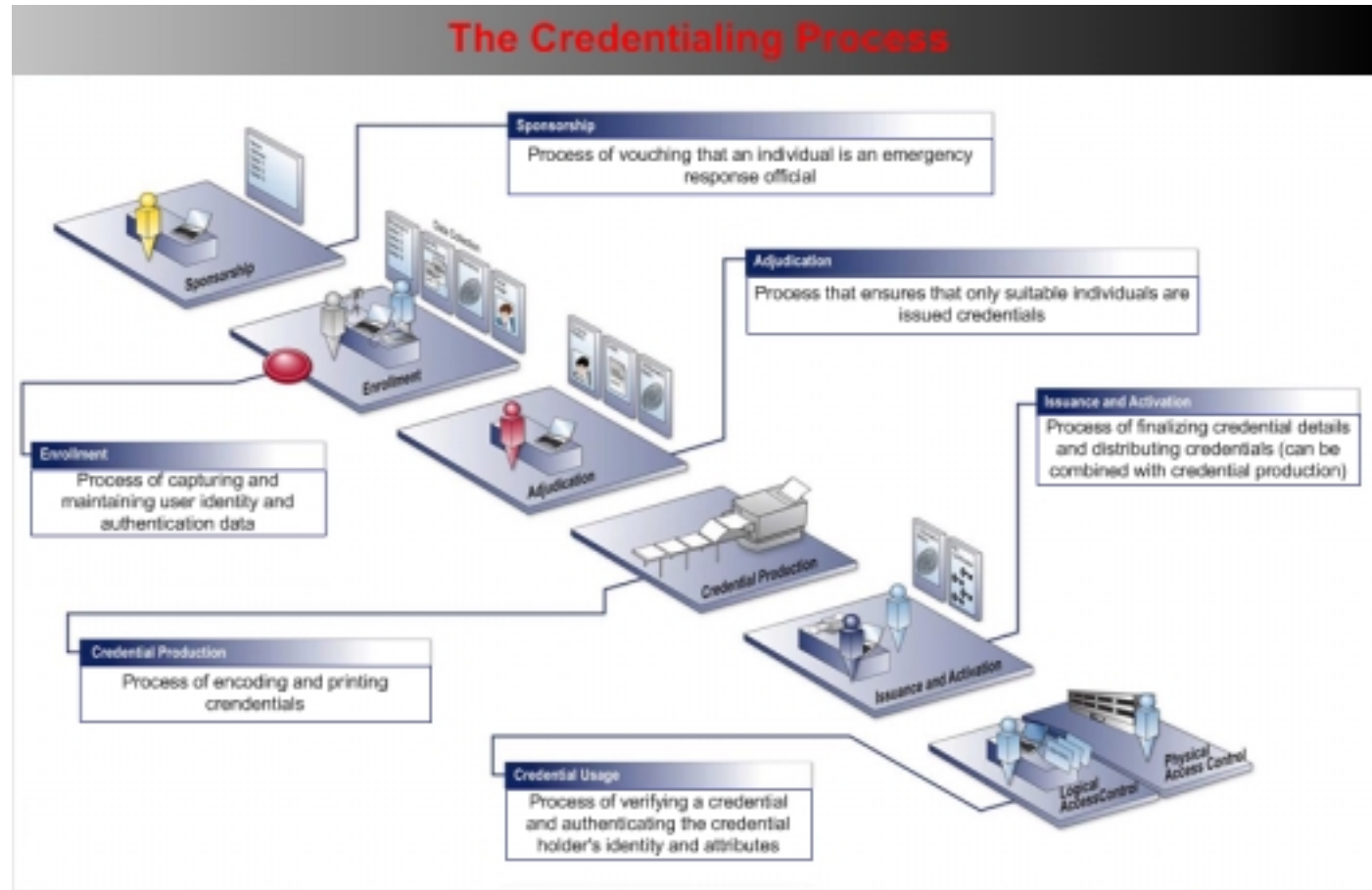
Benefits of the Approach

- **Credential capable of strong authentication**
  - ➤ Essential first step to high assurance enterprise security

- **Commercially available smart tokens use the FIPS 201 standard**

- **Enterprise logical and physical access can use same identity infrastructure**

- **Same infrastructure can be applied to devices**

Benefits of FIPS 201

- **Interoperability**
  - ➢ Defined Process for Credential Security Level
- **Strong Authentication**
- **Information Privacy**
- **Multi-Application Support**
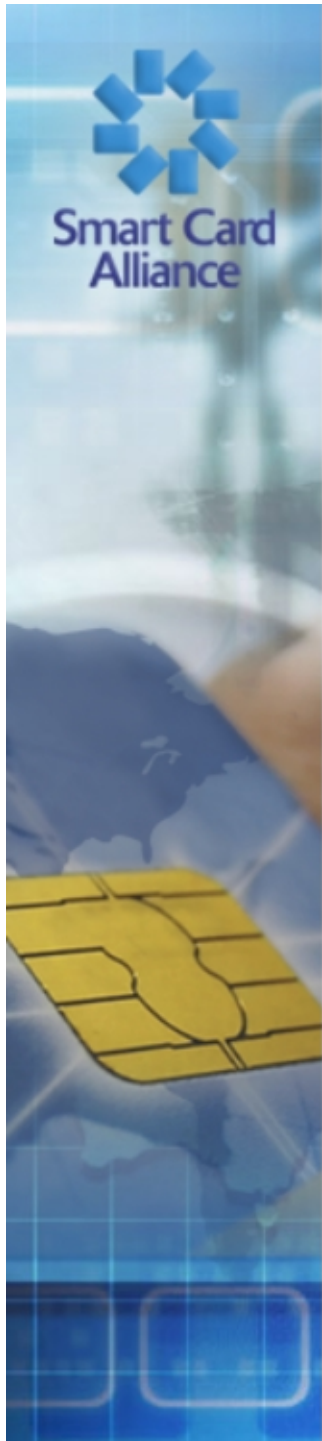- **Standards**
  - ➢ Wide range of suppliers

Use Cases

EQUIPMENT STORAGE

- **Physical Access**
  - ➤ Use it every day!
  - ➤ 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

Use Cases

- **Identity and Attribute Management**
  - ➤ 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
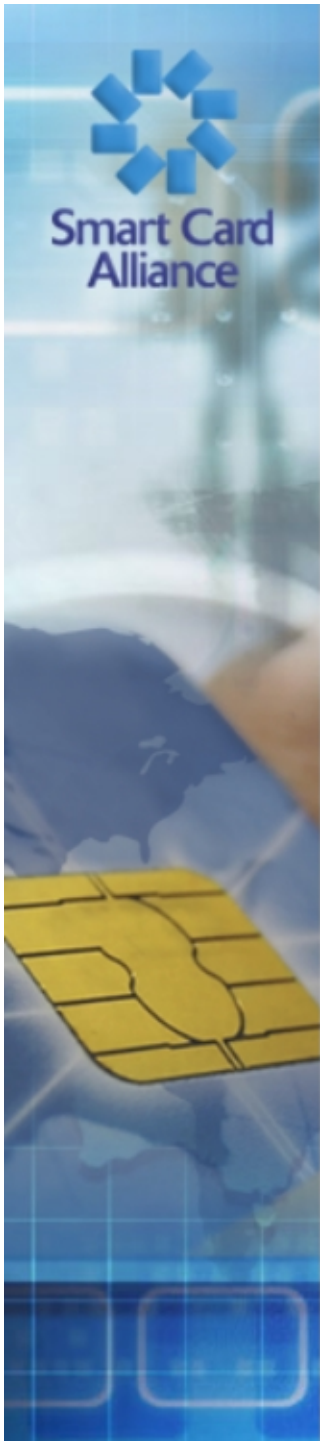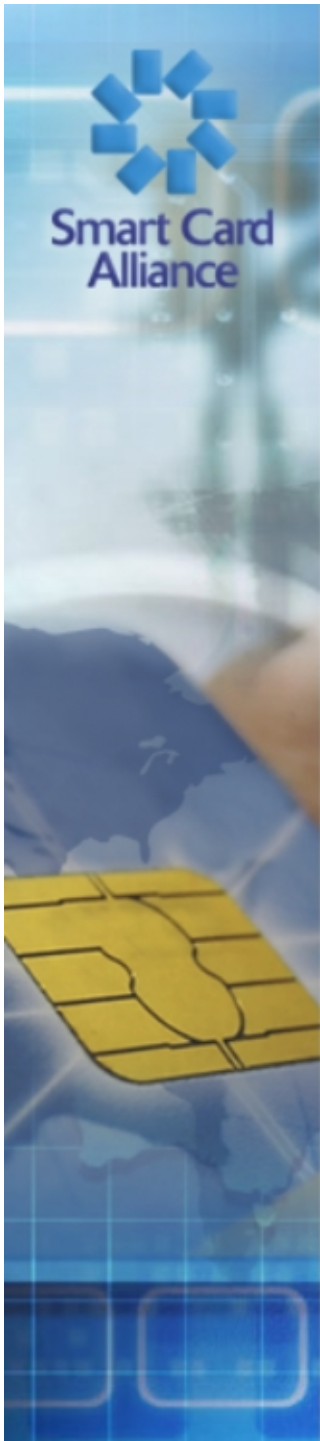
Use Cases
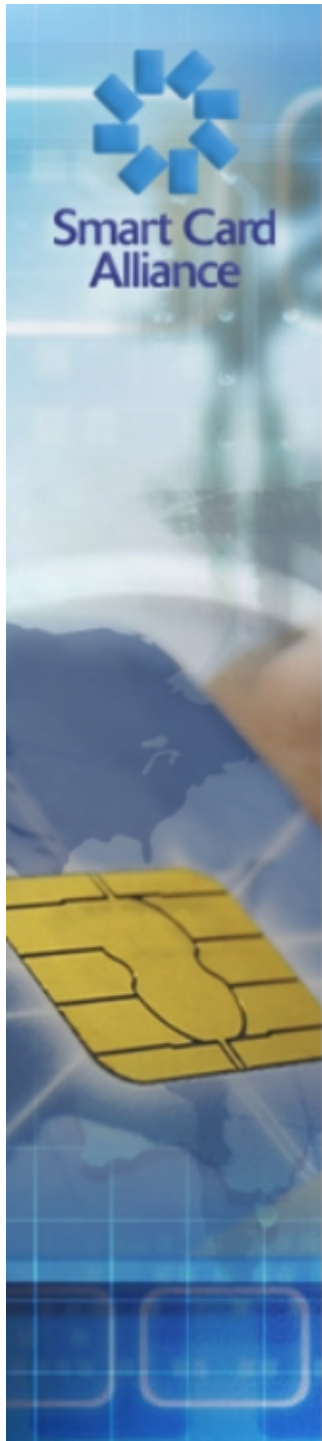
- **Emergency Response**
  - High Assurance and Trusted Identity
  - Incident Scene Access
  - Situational Awareness and Incident Scene Management and Tracking
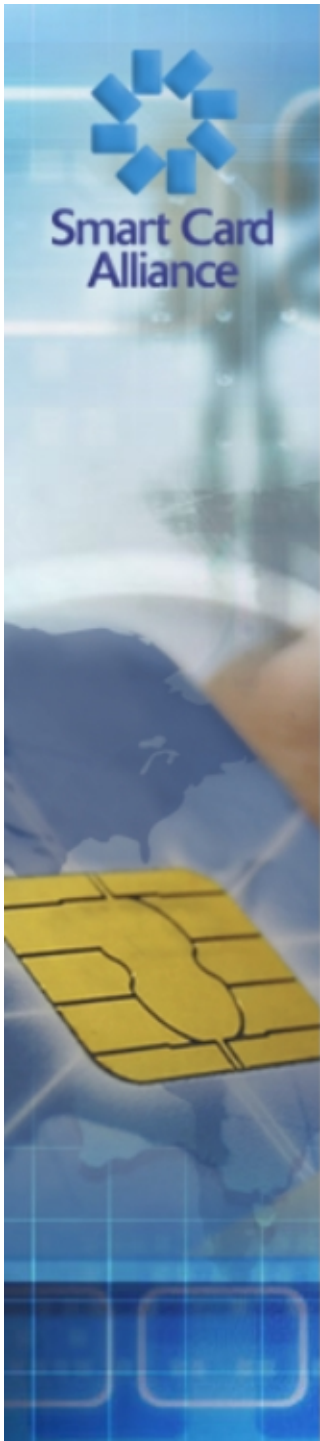 - Just-in-Time Credentials

Use Cases

- **Continuity of Operations & Continuity of Government**
  - ➤ Different from Mutual Aid
    - Security Operations Centers
    - Network Operations Centers
    - Evacuation, Airlift, etc.
    - Critical Infrastructure
  - ➤ Enduring Constitutional Government (ECG)
    - HSPD 20/NSDP 51
      - Relying parties at disaster response and recovery scenes to make authorization decisions
      - Those doing post-event reconstruction (Stafford Act reimbursement)
      - Forensic evidence of those entering hazardous areas
      - Use to improve training for disaster response and recovery in the future.
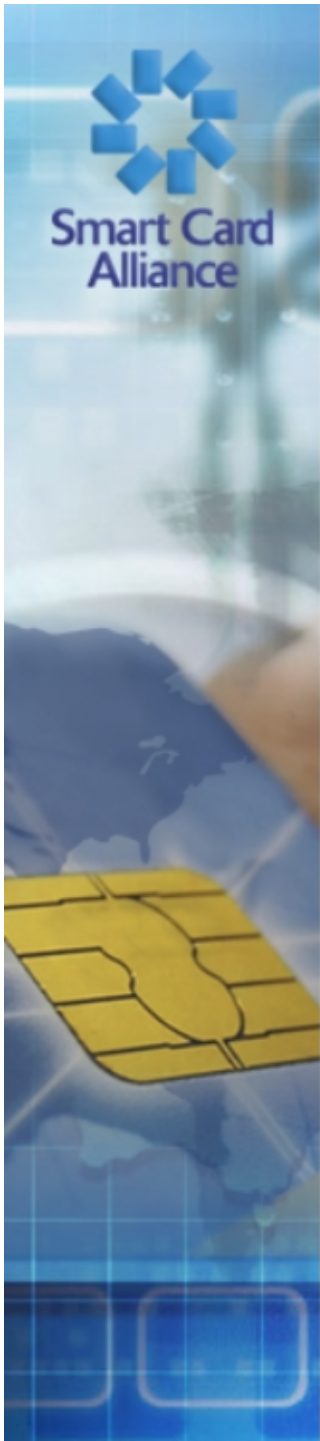
Emergency Response Official (ERO) Credentials

- **Leverage FIPS 201**
  - ➤ Interoperable across jurisdictions
  - ➤ Multi-use
  - ➤ Part of a growing population outside of Federal Employees and Contractors
- **How to issue a credential**
- **What it's used for**
- **Some examples**

Logical Access Control

- **FIPS 201 supports a wide range of applications**
  - Identity Certificate (~PIV Auth)
    - Network Log-on
    - Secure Web-Sites
    - Situational Awareness, Command and Control
  - Card Authentication
  - Digital Signature
  - Encryption

DHS and FEMA

- **Growing communities of interest**
- **Growing number of use cases**
- **Infrastructure for answering the questions based on a FIPS 201 interoperable credential**
  - ➢ FPKI Policy
  - ➢ Trust anchor of FBCA
  - ➢ The challenge /response routine enabled by public/ private key technology application
  - ➢ The linkage of the PIV credential PAK with attributes assigned that select individual
  - ➢ Routine update
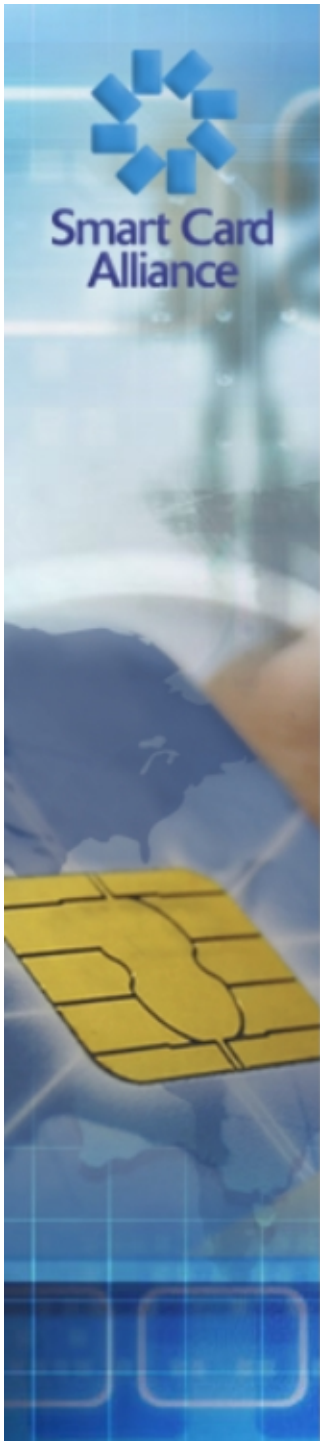
State and Local

- ## VA
  - ➢ Part of initial National Capitol Region deployment
  - ➢ Next phase, broader state deployment

- ## CO, et al
  - ➢ One of several states looking to achieve appropriate security assurance by verifying the claimed identity of individuals seeking access to all-hazard incidents
  - ➢ Secondarily, to communicate the qualifications, skills and training of first responder personnel to the Receiving Authority Incident Command.
  - ➢ Base the program upon recognized standards, open-system architectures, and non-proprietary technologies.