RTV REAL·TIME VERIFICATION

Verification You Can Trust

FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT AND PERSONAL IDENTITY VERIFICATION (PIV) SOLUTIONS

Homeland Security Presidential Directive 12 (HSPD-12), FIPS-201, and the latest Federal Identity, Credential, and Access Management (FICAM) Roadmap and Guidelines provide guidance for Personal Identity Verification solutions that facilitate business between the U.S. Government and its business partners and constituents.

RTV provides an integrated solution for identity management, professional certification tracking, and credential enrollment and authentication in support of federal guidelines and public safety.

Table of Contents

Executive Summary

Situation Overview

A critical threat facing public and private security personnel continues to be unauthorized access to critical infrastructure, sensitive facilities, public events and logical assets.

National Strategy for Homeland Security

- Create Collaboration Mechanisms
- Establish Efficient Information Sharing
- Improve Monitoring Capabilities
- Authenticate and Verify Identities

E-Government and E-Authentication initiatives were tasked with developing a more citizen-centric, efficient, and responsive government. Officials quickly realized that personal identity verification for physical access and logical access was critical to enable trust as well as maintain safety and security.

After 9/11, the Federal Government began formerly addressing the need for a common, trusted basis for digital identity and access management. In 2004, President Bush signed *HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors* mandating a government-wide standard for secure and reliable forms of identification.

> *"The ICAM target state closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing. It also seeks to support the enablement of systems, policies, and processes to facilitate business between the Government and its business partners and constituents."*
>
> --Smart Card Alliance

As investments in identity programs continually accelerate, coordinating efforts among federal and local agencies, in addition to broad-ranging private enterprises, is essential in achieving necessary efficiencies and effectiveness. To help support this mission, the CIO Council established the Identity, Credential, and Access Management Subcommittee to "foster effective ICAM policies and enable trust across organizational, operational, physical, and network boundaries." To support this effort, they created the *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance* (current Version 2.0).

The FICAM guidelines conceptualize a comprehensive and integrated approach to ICAM challenges. *Figure 1 – ICAM Conceptual Diagram* clearly identifies the different stakeholders and functional requirements that must seamlessly interact in order to achieve the desired results.

Federal, state, local agencies must work closely with business partners and citizens ("Federation") to securely and privately share key identity information in support of national security and general public safety.

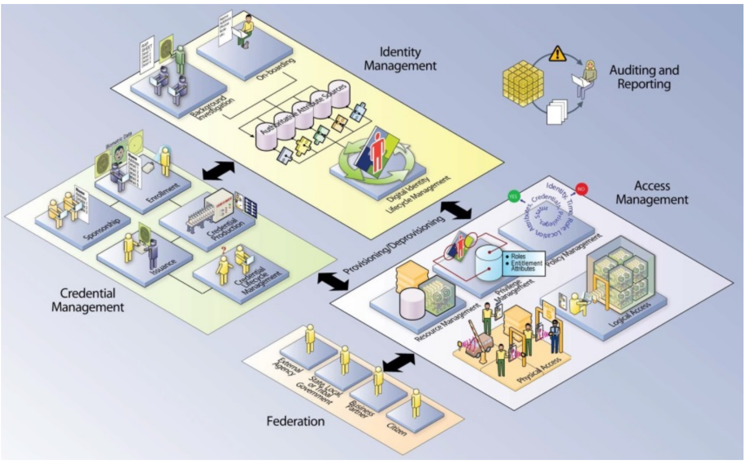


Figure 1 – ICAM Conceptual Diagram

ICAM-compliant solutions must perform enrollment, certification, and credentialing functions with the utmost integrity, assuring known and vetted individuals of unimpeded access to physical and logical resources in accordance with the privileges they have earned and the policies of each unique asset-owner.

The Benefits of ICAM:

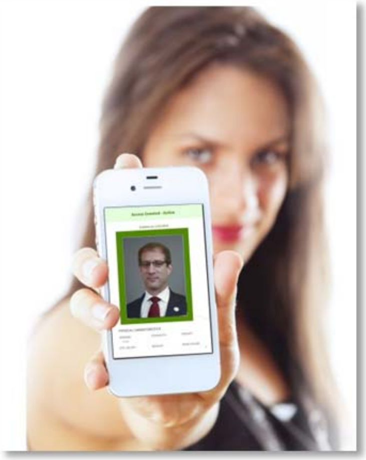
- Increased Security
- Compliance
- Improved Interoperability
- Elimination of Redundancy
- Increase in Protection of Personally Identifiable Information (PII)

A Strategic Vision and Call to Action

Through a series of historic initiatives, government's vision of technology evolved into a strategic new way of operating with a goal of creating a reliable, interconnected, and secure information infrastructure that enhanced the quality of service to the public, made it easier for citizens to interact with the government, improved government's efficiency, effectiveness, and responsiveness.

Advances in information technology, driven by the necessity of improved efficiency, increased automation and interconnectivity. However, these same advances created new vulnerabilities, not only to equipment failure and human error, but also to physical and cyber-attacks. The reality of increased vulnerability created E-Authentication and the Federal Identity Credential Initiative to help create trust and confidence in E-Government. These initiatives laid the groundwork for the *Homeland Security Presidential Directive 12: A Policy for a Common Identification Standard for Federal Employees and Contractors* (HSPD-12).

HSPD-12 is a call to action to create a secure and a reliable identity infrastructure for government employees and contractors. The policy instructs NIST to produce a Federal Information Processing Standard for Personal Identity Verification (PIV). To help protect agencies and departments against terrorist threats and identity theft, the PIV would be used in access applications for Federally-controlled facilities and information systems. Among other things, the resulting FIPS-201 specification creates a standardized, interoperable smart card platform that can make use of Public Key Infrastructure (PKI) digital certificates and biometrics to authenticate identity along with a core set of credential elements.



Although current use continues to grow, PIV "smart cards" have inherent threats that range from improper use of a valid card and the use of counterfeit cards to the use of lower sensitivity-rated cards to gain access to more critical assets.

Additionally there are two challenges that will need to be addressed.

- Establishment of one standard for many decentralized agencies
- Identification of a technology that can drive interoperability among federal, state, local agencies as well as private enterprises.

Real-Time Verification™ (RTV™) is an identity verification, professional certification tracking, and credential management technology that helps mitigate the vulnerability of relying upon smart cards while flexibly meeting the unique challenges set forth in ICAM.

A fully-hosted and managed safety and security solution, RTV supports the secure and interoperable enrollment, vetting, training, and credentialing of organizations and individuals who must comply with Government regulations and/or private customer requirements. Today RTV is used by public agencies, facility owners, unions, and contractors to establish Trusted Communities that help assure the identity, safety, and security of workers who access sensitive facilities and critical incident scenes in support of infrastructure protection and public safety.

RTV's secure, Web-based Trusted Communities enable:

- Sponsorship and enrollment of individuals affiliated with participating organizations
- Collection and validation of identity information including biometric acquisition and authentication
- Processing and management of background screening, professional training, HR and other personal attributes
- Provisioning, issuance, certificate validation, and real-time authentication of ID credentials
- Optimal privacy protection through permission-based controls and comprehensive audit records

Ref: 3

Real-Time Verification (RTV) Delivers Turnkey Compliance

Identity Management

Enrollment

Secure Personnel Enrollment forms provide an easy-to-use, secure method for employees, vendors, and contractors to provide private personal information and vital consent forms required for identity verification and background screening services. The forms, including individuals' digitized signatures, are time-stamped, encrypted, and archived for future reference. All personal information is safe and protected by our audited data security and use policies. Information is shared on a need-to-know basis only.

Pedigree Validation

Pedigree Validation positively identifies all employees, vendors, and contractors to assure that individuals are who they claim to be. Identity verification services match individuals' full name, SSN, date of birth, and address history to reasonably assure identity information

Biometric Acquisition and Authentication

RTV seamlessly integrates legacy access control hardware as well as advanced biometric identity verification technology. Safety officers can biometrically validate credentials with a reader or a smart phone using our Mobile Authentication Tool (MAT).

Affiliation Management

Department affiliation is verified as well as the ability for incident commanders to verify within their expanded mutual aid community. You can instantly benefit from improved participation of your local area to help build cooperation among the nation's first response organizations, public and private.

Skillset Management

Self-Assignment

EPIC's detailed professional training records make tracking of broad-ranging requirements easy. You can 'self-assign' certifications for training provided within your organization.

Third-Party Integration

Effortlessly integrate third-party processors (e.g. training and fitness exam facilities) to enhance operational efficiency and effectiveness for optimal administrative collaboration.

Credential Management

Issuance

Comprehensive member records enable consolidation and simple organization of information sources for identity and biometric data, certifications, and credential issuance and tracking.

Certificate Validation

RTV promotes certificate validation by credentialing upon successful completion of all investigations, training and fitness exams, RTV queues the individual for badge printing within the system to the security management as deemed appropriate by authorizing SOPs.

Secure, Trusted, Reliable Authentication

Flexible user-permission management, easily configurable access control, and dynamic user interfaces that help assure user adoption are RTV's core competencies. We provide another level of authentication that is not easily compromised, altered, or hacked.

© 2013 Real-Time Technology Group

RTV Meets Positive Identity Verification Challenges

RTV was developed by Real-Time Technology Group®, LLC to meet the challenges of Homeland Security and address the market void for a robust technology that could help improve the safety and security of sensitive workplaces.

Because people are the source of both digital and physical threats, clearly and accurately identifying people who have access to a place, object, or information is fundamental. Similarly, everyone who does not have access to a place, object, or information must be identified and rejected. Real-Time Technology Group's core technology was leveraged to provide a unique information-sharing platform in RTV, to meet the diverse needs of facility owner/operators, labor resources, safety and security specialists, and privacy advocates in achieving this goal.

The vision for RTV was to create a flexible information-sharing technology that was easily configured, rapidly and cost-effectively deployed, and interoperable among disconnected business partners and security systems. RTV was designed to quickly and easily verify the identity and credentials of individuals accessing facilities where the protection of workers, infrastructure, and assets is critical. This advanced, permission-based technology enables real-time sharing of Sensitive Security Information (CFR Title 49 Parts 15 & 1520) and Critical Infrastructure Information (CFR Title 6 Part 29?) on a strictly controlled, need-to-know basis.

RTV provides encrypted, Web-based transmission of need-to-know information to individual authorized users in support of collaborative workplace safety and security programs. Only the appropriate and duly- authorized users can maintain worker information including their active credentials. Nationally accredited, independent Third Party Administrators provide investigative, testing, and training services, and this credential information need not ever be disclosed to security personnel. RTV dynamically compares facility requirements to each worker's active credentials, providing security personnel, or an access control system, with a simple green or red light to indicate access granted or access denied. RTV intuitively meets the individual and collaborative security needs of facility owners, contractors, worker organizations and service providers.

Flexible user-permission management, easily configurable access control, and dynamic user interfaces that help assure user adoption, are RTV's core competencies. RTV complements Personal Identity Verification (PIV) systems that promote identity validation, usually in the form of smart cards, by providing another level of authentication that is not easily compromised, altered, or hacked. Additionally, RTV's identity validation can be used in conjunction with, or independently of, personal identification systems including drivers' licenses, organization IDs, and smart cards.

Technology Strengths

RTV is specifically designed to help industries build on existing relationships and service partnerships by enabling their collaborative effort to better control access to sensitive facilities. RTV helps established industry groups to better control and mitigate risk by actively utilizing workers' credentials in day-to-day workplace safety and security programs, setting a new standard for worker identification and credential verification:

- Enables secure information sharing among business partners on a need-to-know basis.
- Protects workers' right to privacy with secure, permission-based access control.
- Easy to implement and easy to use. No special hardware or software to install.
- Comprehensive and fast.

Secure Information Sharing Platform

The EPIC RESPONDERS technology platform enables unique, need-to-know knowledge sharing among facility owners, worker organizations, contractors and service providers to deliver enhanced worker identity verification at workplace entry. The technology allows for uniform, consistent identity and credential authentication. Workers do not require redundant background investigations, fitness testing, or safety training to enter multiple worksites with diverse security requirements. Facilities can better manage site access and critical zones by assigning any number of unique credential requirements for each critical zone within a facility. Additionally, authorized users can schedule and confirm access rights, as well as verify who is on site at any given time. The seamless integration of workers' Sensitive Security Information and facilities' Critical Infrastructure Information offers vastly improved administrative efficiency and record processing and eliminates costly redundant testing, training, and data entry.

Permission-based Credential Management

RTV improves the efficiency and credibility of independent testing and record maintenance. Easy to maintain worker records provide customized information that includes contact information, organization memberships, recent employers, active credentials and recent activity logs. Each worker's sponsor controls access to its workers' records by, easily granting limited permissions as required maintaining comprehensive credentials for workers and ensuring unimpeded access to secure facilities. RTV's unique control over users' permissions enables worker sponsors to continue to rely on nationally accredited, independent Third Party Administrators for investigative, testing, and training services without compromising worker privacy.

RTV never discloses a person's credentials. Security personnel or an access control system, read a simple green or red light to indicate access granted or denied. This intuitive data processing maintains strict confidentiality of personal information while meeting the diverse needs of industry groups, and has proven to be a major factor in earning the trust, approval, endorsement, and adoption of RTV among unions, contractors, construction managers, and facility owners in New Jersey.

Enhanced Real-Time Access Control for Employees, Contractors, and Visitors

RTV's dynamic architecture enables user's real-time control of secured entrance access requirements. Infinitely flexible to meet changing security requirements, RTV presents an integrated view of surety, fitness, safety, and technical requirements for reliable real-time credential authentication at any number of unique security checkpoints. Because RTV empowers interoperable control over geographically dispersed facilities, multi-facility owner/operators can easily set and dynamically change access requirements at any time.

In the case of changing threat levels, security administrators can raise credential requirements for upgraded access verification across any number of secured entrances instantly.

RTV delivers simple point and click control of:

- Unlimited security checkpoints
- Required credentials by location
- Workers currently on-site
- Location activity logs

At any given place and time, RTV identifies access requirements, intuitively scans an individual's active credentials, and within milliseconds confirms whether access rights should be granted or denied. Where exceptional levels of security are appropriate, security administrators can choose to schedule events and instantly set access criteria that limit entry to specific pre-assigned groups or even individual workers. To ensure interoperability and fast, cost-effective implementation, RTV seamlessly integrates legacy access control hardware as well as advanced biometric identity verification technology.

Ref: 3

HSPD-12 Proven Capabilities

HSPD-12: Personal Identification Standard	RTV: Proven Capabilities
Based on sound criteria to verify individual employee's identity	Customized to reflect sound criteria established by user groups such as facility owners, contractors, and worker organizations.
Strongly resistant to fraud, tampering, counterfeiting and terrorist exploitation	128-bit SSL encrypts all data transmissions and redundant physical and logical security products' data sources for state-of-the-art resistance to fraud, hacking, tampering, counterfeiting, and terrorist exploitation.
Personal Identity can be rapidly verified electronically	Intuitive online verification completed in milliseconds provides real-time identity and credential verification.
Identity tokens issued only by providers whose reliability is established by an official accreditation process	Active worker credentials issued by the appropriate worker organization, contractor, facility owner, or nationally-accredited Third Party Administrator in accordance with their official accreditation processes.
Applicable to all government organizations and contractors	RTV provides interoperability among an unlimited number of facilities, organizations, and contractors.
To be used to grant access to Federally-controlled facilities and logical access to Federally-controlled information systems	RTV's worker credential management technology can be leveraged to address both physical access to Federally-controlled facilities as well as logical access to Federally-controlled information systems.
Graduated criteria from least secure to most secure to ensure flexibility in selecting the appropriate security level for each application	Dynamic access credentialing provides virtually infinite flexibility and security control across multiple facilities and work sites.
Protects citizens' privacy	Strictly controlled user access in conjunction with intuitive identity and credential verification procedures protects workers' rights to privacy as well as Sensitive Security and Critical Infrastructure Information.

The success of smart PIV cards to help implement a common identification and security standard for Federal employees and contractors will depend upon:

- Combining with a number of ID system technologies such as biometrics and digital certificates
- Sharing a permission-based infrastructure that supports a common trust level
- Utilizing a technology that enables their implementation within a single group, across multiple groups or enterprises or among multiple organizations or enterprises.

RTV provides the robust technology that supports the identity management that a smart PIV card must provide.

Ref: 3

RTV Helps Mitigate Threats

No technology can claim to be foolproof. EPIC RESPONDERS can help to reduce threats to the proposed Personal Identity Verification (PIV) Standard. The overall threat to a PIV system is: Unauthorized access to physical facilities or logical assets under its protection. As a Web-based credential management technology, EPIC RESPONDERS can effectively respond to the traditional vulnerabilities PIV systems face.

Top Issues and Challenges Facing PIV Systems

PIV Vulnerabilities	Closed Systems' Response	RTV Response
Improper Issuance	▪ Use of source documents ▪ Application by accredited ▪ Sponsor ▪ Controlled issuance process	▪ Application and data entry made by accredited sponsor eliminates redundant data entry. ▪ Access control utilizes identity and credential data verified independently of holder's smart card.
Counterfeiting	▪ Holographic organization seal of issuer ▪ ID or Serial Number burned into chip ▪ Encryption of stored information ▪ Integration of PIN with cryptographic authentication	▪ All of the traditional countermeasures can be compromised whether a holograph or a PIN number is used. ▪ RTV's technology intuitively scans multiple identity and credential references to authenticate card holders, including traditional images and biometrics. ▪ All data transfer is encrypted and securely stored.
Stolen or Borrowed Card to Gain Access	▪ Card accountability procedures (i.e., reporting/publication of lost card lists) ▪ Use of biometrics ▪ Visual inspection of card holder image with card presenter	▪ Lost cards can be immediately revoked and rendered inoperable across any number of disconnected agencies and departments. ▪ Access control utilizes identity and credential data verified independently of holder's smart card adding another physical and logical dimension to verification of individual access rights. ▪ Independently stored traditional and biometric images help mitigate risk associated with lost or stolen cards.
Identity is not sufficiently verified in most ID Systems	▪ Use of passwords	▪ Passwords represent security risk because they are usually controlled by the user who can easily guess passwords or share passwords with others. ▪ RTV's identity and credential verification process is not password driven
Use of Card Issued for Access to Lower Sensitivity/Critical Assets to Gain Access to More Sensitive/ Critical Areas	▪ Electronic credentials for each level authorized ▪ Color coding or pattern changes on physical card to indicate levels	▪ RTV provides virtually infinite flexibility for determining access requirements in critical zones within any number of facilities. ▪ Access rights can be granted at a group level or uniquely configured to meet individual needs without requiring special markings or visual indicators that can easily be replicated or faked.

Ref: 3

Proving the true identity of a person seeking verification	▪ Applicants for cards can misrepresent their identity ▪ when seeking employment	▪ Information sharing enables the appropriate worker sponsor or their appointed and nationally-accredited Third Party Administrators to provide appropriate levels of identity and credential verification as required by disconnected agencies, department, and business partners.
Identity credentials can be difficult to issue and manage for large populations	▪ Passwords must be reset	▪ Worker identity and credentials can easily be maintained by a worker's primary sponsor yet shared as required by secondary agencies, departments, and business partners, drastically reducing the administrative effort required to ensure proper access rights and unimpeded workplace access.
Different agencies /departments require their own identity documents causing employees to carry multiple IDs	▪ Employees carry multiple IDs to access other agency facilities and to access computer networks	▪ RTV provides single card interoperability among disconnected agencies, facilities, and computer networks to intuitively interpret access rights based on unique facility requirements.
Current ID Systems are expensive to operate and support	▪ Cost of configuring and maintaining passwords can range from $100 to $350 pp/py	▪ RTV is a cost-effective, rapidly deployable, comprehensive identity and credential verification solution.

Conclusion

RTV technology is the technology solution that can encompass all of the components and processes that effectively support the implementation of a Personal Identity Verification standard for Federal employees and contractors. From maintaining worker privacy to ensuring interoperability among disparate databases, RTV technology can provide significant efficiencies to meet the security challenges today among Federal agencies and Departments and the interoperability capabilities to expand these efficiencies to meet the security challenges well beyond.

For more information, please visit our Website at: www.realtimetg.com/rtv.

© 2013 Real-Time Technology Group

Appendix

Corporate Background – Expert Managed-Solution

Real-Time Technology Group (RTTG) has specialized in developing and hosting web-based critical information management systems since 1999. Our proprietary systems and infrastructure are routinely audited due to our active work in support of security procedures at World Trade Center and NY/NJ transportation infrastructure. Vigilant support of our security and continuity of service responsibilities are paramount at all times.

We maintain a deeply experienced staff that includes subject matter experts with individual specialties in logical security, network engineering, database design, programming and administration, application architecture, and web development. Our technologists *average* 18 years in their respective expertise, and our leadership team joined the company more than 10 years ago.

Our network and server infrastructure is housed in a secure, protected, environmentally-controlled, and audited SSAE 16 SOC 1 Type II facility in eastern PA, a short distance from our corporate headquarters in west-central NJ. Operated by Windstream, the data center features: guarded access control; “blipless” power supply backed up by UPS and generator power; redundant climate control; non-toxic and waterless fire suppression; and, multiple fiber connections to major switching centers in PA, NY, and NJ.

Inside, RTTG’s private network and hosting infrastructure features fully-redundant network and security appliances, separate application and database host-server clusters, and state-of-the-art SAN storage arrays. In addition, we maintain an “old-school” physical server environment consisting of domain controllers, web and database servers in the unlikely event our virtualization platform is rendered inoperable.

RTTG is prepared to execute the following Scope of Work, building, deploying and maintaining application and database servers to host BPASCS’s Identity, Certification Tracking, and Credential Management solution in support of school safety and security operations as required deemed appropriate by BPASCS. In doing so, BPASCS can be assured of continual best-in-class physical protection, logical security, fault tolerance, and technical maintenance and support of its security operations.

REAL·TIME TECHNOLOGY GROUP
Critical Information Management

RTV IDENTITY MANAGEMENT SOLUTIONS

- ✓ 2,035 Felons Disqualified
- ✓ 303 Fraudulent Identities Turned Away
- ✓ 8 Open Wants, Warrants or Indictments Identified
- ✓ 5 Identity Thieves Apprehended
- ✓ 6 Illegal Aliens Deported

They’re not working at our critical infrastructure. What about yours?

© 2003-2013 Real-Time Technology Group. Patents Pending. All Rights Reserved.   www.realtimetg.com

Publication Acknowledgements

"Announcing the Personal Identity Verification for Federal Employees and Contractors." *Federal Information Standards Processing 201*. (Version 1.0) Public Draft; 2005.

Bush, President George W. *Homeland Security Presidential Directive/Hspd-12*. Washington D.C., August, 2004.

E-Government Strategy Implementing the President's Management Agenda for E-Government. Washington, D.C., 2002.

Federal Identity Credentialing Committee. "Policy Issuance Regarding Smart Cards Systems for Identification and Credentialing of Employees." March 2004.

Forman, Mark. "Streamlining Authentication and Identity Management within the Federal Government," *Memorandum for The Chief Information Officers of Departments and Agencies*. Washington, D.C.; July 2003.

"HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors, Information Assurance and Critical Infrastructure Protection: 'A Federal Perspective'." Presented by Government Electronics And Information Technology Association; 2001.

Messmer, Ellen. "Feds eyeing one access model for all." *Network World*. September 2004.

"Personal Identity Verification (PIV) for Federal Employees and Contractors: FIPS PUB 201." (Version 1.0) Public Draft; US Department of Commerce. To be issued February 25, 2005.

Personal Identity Verification System: Identity Verification Cards.
Note: This document is based on a publication of the Smartcard Alliance. See listing below

"Policy Issuance Regarding Smart Card Systems for Identification and Credentialing of Employees," Federal Identity and Credentialing Committee. February 2004, available at www.smartcard.gov/smartgov/information/scpfinal2004.doc

"Secure Identification Systems: Building a Chain of Trust." Smart Card Alliance, 2004.

"Securing card issuance, government smart cards, and biometrics in '05." *RFID News*; available at www.rfidnews.org

Spencer, Judith, GSA; Barker, W.Barker, NIST; Louden, Chris, Enspier Technologies, "Federal Identity Credentialing & E-Authentication: An Update." December 2004, available at www.egovi.com

Web References

http://csrc.nist.gov/piv-project

www.egov.com

www.whitehouse.gov

www.mipt.org/Presidential-Decision-Directives

www.smartcardalliance.org/industry