

Personal Identity Verification (PIV) and
Personal Identity Verification Interoperability (PIV-I)
Strategic and Tactical Consulting Services

January 2010



1264 Beacon Street, #5

Brookline, MA 02446

+1 617.201.4809

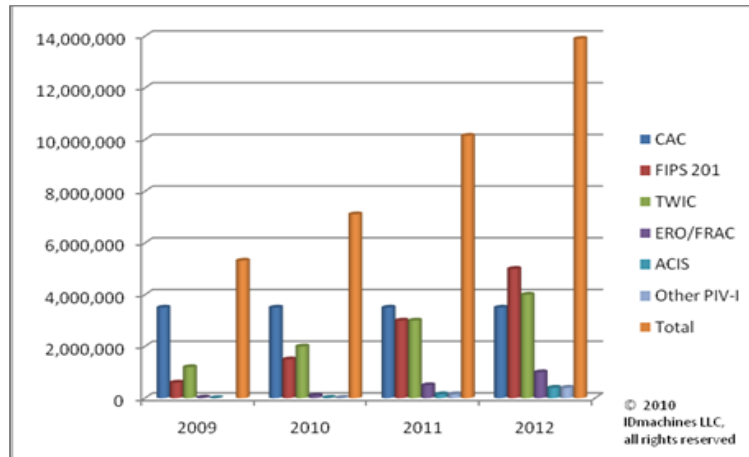
<http://www.idmachines.com>

<http://idmachines.blogspot.com>

Introduction

IDmachines provides strategic and tactical consulting products and services for the identity infrastructure market leveraging the specifications set by the National Institute of Standards and Technology (NIST) [Personal Identity Verification \(PIV\) program](#). These services also apply to those outside of the Federal government to leverage the standard to provide [Personal Identity Verification Interoperability \(PIV-I\)](#) identities to their organizations.

Why has IDmachines focused on this particular business proposition? Trusted identity of employees, contractors, vendors and network devices has always been a crucial part of any enterprise's security solution. More recently identity theft, identity fraud, mobile and remote workforces and distributed enterprise facilities has placed a premium on the need for modern identity and access control solutions. The PIV and PIV-I standards enable the use of a single multipurpose identity credential for logical and physical access. It also provides a basis for device authentication. Over 5 million credentials were deployed by the end of 2009 in the United States and this number is expected to more than double over the next 3 years as shown in the following chart¹.



PIV and PIV-I credentials brings numerous economic, privacy and security benefits to the table including; highest possible strength of authentication, commercial off the shelf solutions that can be integrated to meet customer needs, multiple solution sources, flexibility in solution scale from small enterprise to population scale deployments, reduced administrative costs, reduced capital expenditures, increased collaboration with vendors and partners, and enabling workforce mobility, to highlight a few.

To briefly review how we arrived in this situation let's quickly look over the last ten years. The use of smart cards by the United States government began in earnest with the deployment of the Navy Smart Card around 1999. This evolved into the Department of Defense Common Access Card (CAC) which is currently deployed to approximately 3.5 million individuals. In August of 2004 [Homeland Security Presidential Directive 12 \(HSDP-12\)](#) was signed mandating a common identity vetting and issuance process and the use of a multi-purpose smart card for access to United States government facilities and

¹ Estimates based on <http://www.fedidcard.gov/> , <http://twicinformation.tsa.dhs.gov/twicinfo/index.jsp> and other sources (e.g. DoD CAC, PIV-I deployments)

networks. Importantly this means that any PIV or PIV-I card issued to any employee or contractor can be used to permit access. There are now over 5 million credentials that leverage this approach.

In addition to our federal government this standard has been used to develop solutions for critical infrastructure. These other programs include the [Transportation Workers Identification Credential \(TWIC\)](#), Airport Credential Interoperability Solution (ACIS), emergency response official (ERO) and [first responder authentication credential \(FRAC\)](#) and by state and local governments. The standard has been adopted by [public safety agencies in the United Kingdom](#), by an aerospace consortium via [CertiPath](#) and the [Transglobal Secure Collaboration Program \(TSCP\)](#), by the pharmaceutical industry via [SAFE/Bio-Pharma](#) and so PIV and PIV-I use continues to evolve and expand.

IDmachines works with its customers to use these standards based solutions across government, critical infrastructure and any organization that wants to benefit from a single high assurance multi-purpose identity credential. As a result IDmachines has developed a number of offerings to help organizations take advantage of this important development in the identity, access and security world.

Services

IDmachines services vary by the type of customer organization. These organizations typically fall into the following categories: Manufacturers, System Integrator and End-Users

Manufacturers

IDmachines provides manufacturers with strategic and sales consulting services.

Manufacturer Strategic Services

IDmachines manufacturer strategic services include:

- Business plans and business planning
- Executive coaching
- Fundraising and investor support
- Market and competitive research
- Technology assessment and technology transfer
- Product architecture and product roadmap support
- Product approvals

Manufacturer Sales Services

IDmachines manufacturer sales services include:

- Sales plans and sales planning
- Targeted account sales
- Channel sales strategy and channel sales management
- Contract vehicles and schedules
- Partner strategy
- Public relations and marketing support

System Integrators

IDmachines provides system integrators with strategic and sales consulting services and product solutions.

System Integrator Strategic Services

IDmachines system integrator strategic services include:

- PIV and PIV-I Boot Camp
- PIV and PIV-I Check-up
- Business plans and business planning
- Executive coaching
- Fundraising and investor support
- Market and competitive research
- Technology assessment
- Vendor assessment
- Solution architecture

System Integrator Sales Services

IDmachines system integrator sales services include:

- Sales plans and sales planning
- Targeted account sales
- Bid/proposal strategy, preparation, presentation and teaming
- Support for system design, build, installation, operation and maintenance
- Contract vehicles and schedules
- Partner strategy
- Public relations and marketing support
- PIV and PIV-I (logical and physical) solution components (e.g. credentialing, readers, mobile devices, access control and identity and public key infrastructure).

End-users

IDmachines provides end-users with enterprise consulting services in the areas of security, access, credentialing, video, biometrics, sensing, automation and machine learning. These include program management, acquisition, as well as security system assessments, audits and designs.

PIV and PIV-I Bootcamp

IDmachines PIV and PIV-I bootcamp provides customers with a methodology to adopt and use PIV and PIV-I identity infrastructure, credential, access and related applications. The methodology includes:

1. Evaluation of the requirements for issuance of PIV, PIV-I and PIV-C credentials and roadmap for issuance if necessary.
2. End point ability to talk to the PIV credential via its contact and contactless interfaces as well as use any other features presented by the card topology (e.g. bar code and magnetic stripe).
3. Determine the ability of the PACS to do the processing required across authentication methods. In particular this includes the ability to do a challenge and response of the digital certificates and the ability to verify the digital signatures used to provide data integrity. This fundamentally includes an analysis of all system components to address not only process but also word length (e.g. bit lengths). This becomes crucial in a PIV-I environment in order to avoid collisions (two or more credentials treated as the same) as well as addressing cryptographic challenge and signatures as previously mentioned.
4. Determine the ability to validate credentials by taking advantage of the infrastructure mandated under FIPS 201 as well as the need to trust externally issued credentials that are cross-certified to the Federal Bridge Certificate Authority (FBCA). The IDmachines' team members have been at the forefront of the implementation of the On-line Certificate Status Protocol (OCSP) as represented in the request for comment 2560 (RFC 2560) and the Server-based Certificate Validation Protocol (RFC 5055).
5. Provide the proper authorizations using the PACS and personal of end-users enterprise to eliminate unauthorized access to facilities and assets. This includes visitor management as well as emergency response and continuity of operations and continuity of government requirements.
6. Make sure that the PACS meets the enterprise requirements related to logical access control and information security.
7. Develop administration, authentication, authorization and audit (4A) policy, methods and system that streamline compliance requirements and protection of personally identifiable information (PII).
8. Meet the ultimate goal of making security a critical business process that enables enterprise goals and improves the productivity of members of the security team as well as employees, contractors, vendors, business partners and customers.
9. Examine and where necessary enable the use of service or cloud computing based options as part of the migration plan and with it the associated operational benefits.