LS3 Technologies MAKING IT PRACTICAL

Federal Identity Credential and Access Management (FICAM), the 'Cloud', and Cloud Email

INTERESTING THING THIS 'CLOUD'?

The term 'Cloud' is perhaps the most overused and misapplied term in Information Technology today. Where you ask 10 IT professionals "*what is the cloud?*", you are likely to get 15 or more answers, and with a little luck one of them may even be close to accurate. Cloud computing is defined by the National Institute of Standards and Technology (NIST) as, "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1]

IT *buzzwords* like "*go to the Cloud*", "*Service in the Cloud*", and "*Computing in the Cloud*" are highly sought after staples in marketing campaigns. They spawn a number of anecdotal terms, acronyms, catch phrases, and quips in common everyday tech-language that accomplish two things. First, they ensure no one knows exactly what anyone else is really talking about. Second, they permit repackaging of already existing capabilities, services, and applications with new branding and spin to establish an almost fervorish hype. The results are market conditions that incite Agencies to align their Program and Operating Budgets as quickly as possible to get in on the latest "*silver bullet*" that will "*resolve all of their mission critical problems*".

In recent years, Agencies have sought to lower their Total Operating Costs (TCO) by leveraging 'Cloud' based offerings/capabilities. Whether it is getting in on Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Software as a Service (SaaS), or Security as a Service (SECaaS), Agencies offer rudimentary discovery and investigation so as not to be left behind on the latest wave of technical advancement or maturity. As with other buzzword IT management practices, this can result in a temporary displacement of organizational risk through an almost natural redefining of existing problems or arguments; however without appropriate due diligence and analysis, it will also likely instill new constraints, problems, or challenges for the Agency to face. In addition, Agencies are likely to introduce gaps to existing strategic plans as a function of problem redefinition processes – not just encounter risks from non-obvious gaps introduced from new approaches to resolving existing problems. The mathematical formula that represents this market hysteria is:

Disparate/Disjointed Business Problem + Bright Shiny New Technology = New Expensive Old Business Problem

This isn't to say that Cloud Computing is *without value*. There are certainly marked advantages to engaging these capabilities and services to address Agency needs. There are also significant cost savings that can be realized by adopting mature, well defined, and well thought out services or capabilities. This is especially true when you examine the primary characteristics of a "cloud service", which are:

[1] Source: Special Publication 800-145 – The NIST Definition of Cloud Computing

- It is sold on demand – with plans that charge by the minute, hour, month, or year;
- It is elastic – Agencies can utilize as much or as little of the service as they want at any given time;
- It is fully managed by a Provider (the consumer needs nothing but a personal computer and Internet access).

The concern is what and how much is engaged; how these services are to be managed effectively; and what is the exit plan after making the leap and adopting services or capabilities (*assuming one even exists*). In addition, once engaged, what non-obvious gaps exist in service management and which of the Agency problems remain unresolved as a factor expectation not meeting up with reality.

WHAT IS FICAM?

Following the publication of HSPD-12, the National Institute of Standards and Technology (NIST) published the standard with Federal Information Processing Standard 201-1 (FIPS 201)[2]. This standard was augmented with additional technical and operational guidance through the NIST 800 Series Publications[3]. These documents provide a definition for the base components and operational processes that must comprise an HSPD-12 solution. Subsequent to the publication of these standards, the Federal CIO Council published guidance in May 2009 related to PIV interoperability[4]. This publication serves as definition for PIV-Interoperable (PIV-I) credentials for non-Federal issuers (NFIs) such as State, Local, other Jurisdictional governments and private sector or commercial organizations.

In parallel to advancements with standards-based *Credentials*, the Federal CIO Council's Information Security and Identity Management Committee (ISIMC) established the Identity, Credential and Access Management (ICAM) Subcommittee in 2008. This Subcommittee was tasked to align Identity Management activities of the US Government. The Federal CIO Council and the Office of Management of Budget (OMB) worked in collaboration on the establishment of *OMB M-11-11 – Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors*. This Directive requires that Agencies develop and issue an implementation policy, by March 31, 2011, through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems. This policy requires the clear and unambiguous identification of an "*Agency Lead Official*" to ensure the issuance of the agency's HSPD-12 implementation policy[5]. The following specific requirements were established for Agencies as a result of this Directive:

- Effective the beginning of FY2012, existing physical and logical access control systems must be upgraded to use PIV credentials, in accordance with NIST guidelines, prior to the agency using development and technology refresh funds to complete other activities.
- Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation. In order

[2] http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[3] http://csrc.nist.gov/publications/PubsSPs.html

[4] Personal Identity Verification (PIV) Interoperability For Non-Federal Issuers, May 2009 (http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers_May2009.pdf)

[5] Required no later than February 25, 2011 per this mandate

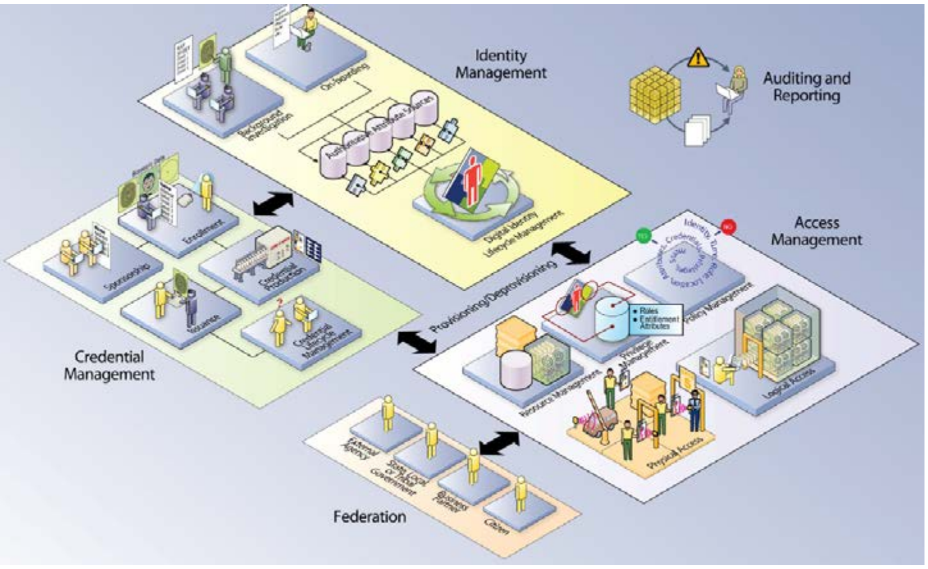
©2013 LS3, Incorporated.

to ensure government-wide interoperability, OMB Memorandum 06-18, "Acquisition of Products and Services for Implementation of HSPD-12" requires agencies to acquire products and services that are approved as compliant with Federal policy, standards and supporting technical specifications.

- Agency processes must accept and electronically verify PIV credentials issued by other federal agencies.
- The government-wide architecture and completion of agency transition plans must align as described in the Federal CIO Council's "Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance" (available at www.idmanagement.gov).

To assist Agencies further, the Federal CIO Council published the FICAM Roadmap and Implementation Guidance[6], which offers prescriptive information for Agencies to utilize in their FICAM planning and execution of implementation plans.

FICAM solutions are predominately based upon enterprise Identity and Access Management (IAM) solutions, with the notable exception of the inclusion and emphasis on *Credential* components. IAM solutions have been in existence for many years, and have been implemented and utilized within the private sector to address identity and security management lifecycles with a significant amount of success. The results of this are a thriving industry with many available COTS products that can be utilized to address the demands of FICAM. Industry market analysis firms provide regular updates, assessments, and opinions as to the maturity, capability, and flexibility of these COTS product offerings, which Agencies can utilize as a means to "jump start" FICAM Programs. In addition to private sector solutions and capabilities, the Federal CIO Council has provided information in various publications that extol a specific Federal Segment Architecture for FICAM. The most commonly distributed illustration for FICAM is sourced from the FICAM Roadmap and Guidance document, which is as follows:

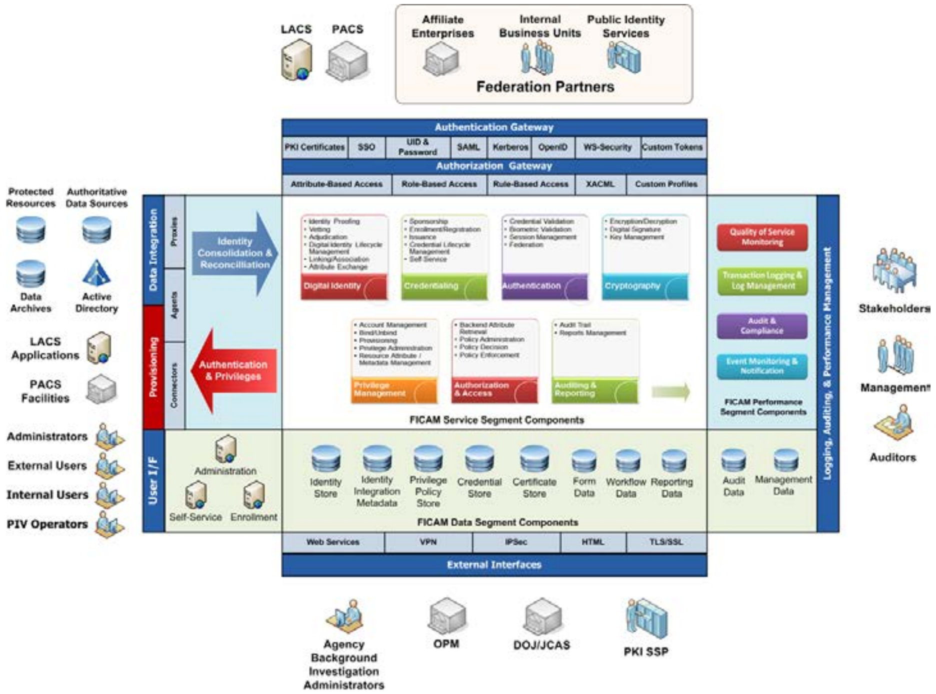


This illustration is typically utilized as a high-level overview of the complementary nature of different parts of ICAM and how concepts once viewed as stove-pipes can intersect to provide an

[6] http://www.idmanagement.gov/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202.pdf

©2013 LS3, Incorporated.

enterprise capability that offers value to Agencies. Additional illustrations and information has since been circulated within government to further describe FICAM in more intricate detail. Consider the following illustration that seeks to decompose FICAM even further into the solution components, processes, and communities of interest that fall within the scope of the FICAM Segment Architecture:



With all of these referenced materials, there exists sufficient information to offer a foundational understanding of FICAM technologies, processes, and practices, and insight into the business value that can be realized from these enterprise-level efforts.

WHAT IS CLOUD EMAIL?

Cloud email can arguably be defined as IaaS or SaaS, depending on email features utilized by the Agency users. The most common definition is that email is an Infrastructure capability (i.e., IaaS), in recognition of email being the most common business service utilized by organizations today, and thereby making it a staple of IT infrastructure capability. To avoid arguments on this point, Service Providers have taken to defining Cloud email using the term, *Email as a Service*, and even adopting its own special acronym: <u>*EaaS*</u>. *After all, the last thing anyone wants in the middle of the sales process is an argument, and the core objective is to maintain focus on securing the sale for a marketable commodity or capability*.

Service Providers leverage common infrastructure and software investment to enable "on demand" email capabilities as an EaaS offering. By leveraging this common investment, EaaS is typically a multi-tenant offering, with more than one Agency taking advantage of economies of scale to drive down Agency subscription costs, and to minimize Service Provider investment need to allow for competitive pricing within the offer. Services are provided over the Internet using standards based protocols that are commonly supported in major email applications and software suites. Based on this, EaaS can be defined as: vendor-offered, multitenant, Internet-delivered service capabilities that are provided with notable scalability and flexibility on a subscription basis.

©2013 LS3, Incorporated.

VENDOR QUALIFICATIONS

Any vendor that wants to succeed in the management, planning, sustainment, or operations of HSPD-12 (*as well as ICAM*) technical frameworks must be dedicated to engaging industry and keeping pace with the evolution or changes associated with these technologies.

The GSA has established a certification program that reviews capabilities of industry vendors, and which results in a certification in HSPD-12 capabilities across a number of service categories. This program was established as a result of Directives such as: *OMB M-05-24 Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* and *OMB M-06-18 Acquisition of Products and Services for Implementation of HSPD-12*.

Important to note with regard to certified vendors is the Service Category they are assigned, ensuring that a *Certified Systems Integration Services and Products* vendor is used for these efforts. This is because the other categories of service (e.g., *Activation and Finalization Services and Products, Card Management and Production Services and Products, Enrollment and Registration Services and Products, Systems Infrastructure Services and Products*) are not as directly applicable to the experience, capability, and talent needed to succeed with migration and transition efforts. The *Certified Systems Integration Services and Products* vendors are more apt to address the integration requirements, end-to-end solution expertise, and direct technical capabilities needed for migration success.

Federal acquisition rules and laws require the use of Qualified or Certified vendors to address HSPD-12 related work efforts. Agencies can opt to engage the GSA Schedule 70 within Special Item Number 132-62 to acquire these resources or at a minimum must utilize the certified labor as listed on the ID Management web site (www.idmanagement.gov) within the acquisition process.

White Paper Author

LS3 Technologies is an organization that has been dedicated to the advancement, use, and practical application of HSPD-12 and ICAM for more than a decade. We specialize in researching, reviewing, and assessing each of the component technologies that comprise ICAM and HSPD-2 solutions. We dedicated significant corporate resources to finding and retaining talented industry experts that share a similar interest in investing themselves in these technologies to offer best-in-class solutions for our customers. Our best-in-class service capabilities have addressed the solution design, development, integration, and operational sustainment needs of PIV and FICAM for a decade.

LS3 Technologies, a valued partner, minority woman-owned 8(a) certified and Small Disadvantaged Business, specializes in full lifecycle IT solutions. Clients benefit from our solid reputation for rapidly and successfully implementing best-in-class practices, processes, and systems. We strive to offer an accelerated return on our customers' time and investment. We carefully select each team member to ensure the resources each provides matches or exceeds expectations of our customers. Our teams of experienced critical thinkers are results-oriented people that cover the full spectrum of the IT industry, with specialized focus areas dedicated to success in individual tasks, yet integrated to keep their eyes on the end state desired. Our cross-functional management approach permits emphasis of strengths within each team member while ensuring a collaborative and inclusive atmosphere for achieving results and making progress.

©2013 LS3, Incorporated.