



The Comments of Brivo Systems, LLC
On FICAM Version 1.0

FICAM and Software as a Service

SaaS and the efficient realization of FICAM goals

by Steve Van Till
President & CEO
Brivo Systems



Table of Contents

Introduction	2
FICAM and Physical Security	3
SaaS and FICAM	4
SaaS Maturity and Multi-Tenant Software Architectures	4
SaaS and Physical Access Management	5
The Emergence of Security-as-a-Service	5
Relevance of Security-as-a-Service to ICAM Goals	5
Role of Standards	6
Cloud Security & PII	9
Cost of Computing Infrastructure	10
Cost of FISMA Compliance	10
Conclusion	11

Introduction

The recent publication the FICAM roadmap¹ is bringing much needed change to the world of physical and logical security, both within the federal government and beyond. In the midst of a “constantly shifting threat environment” in which “data breaches are all too common, identity theft is on the rise, and trust relationships are enforced in an inconsistent and hard-to-understand manner” there is a clear need for a roadmap that will provide consistent guidance with respect to policies, technologies, and standards.

The November, 2009 publication of Version 1.0 of this roadmap represents a significant step toward the goal of leveraging “digital infrastructure to securely conduct business electronically between Federal agencies, their business and coalition partners and with the American public, by promoting the use of authentication, digital signature, and encryption technologies.” As the report further notes, “increasing emphasis has also been placed on improving the physical security of the hundreds of thousands of facilities that the Federal Government owns and leases to support the diverse mission work of its agencies.”

At the same time that the federal government has been engaged in this effort, the IT sector has seen the emergence of a new paradigm in the delivery of software services; namely, “cloud computing” or Software-as-a-Service (SaaS). Physical security providers have been quick to adopt these underlying technologies and leverage them for a variety of new offerings collectively known in the industry as *Security-as-a-Service*.

In preparation for the issuance of the next version of the ICAM roadmap, the ICAMSC has requested input from the public regarding Part B, Implementation Guidance. As the first company to introduce Software-as-a-Service Physical Access Control Systems to the industry in 2002, Brivo Systems is uniquely positioned to provide relevant commentary based on our eight years of serving this segment and observing the changing trends in adoption of this new paradigm.

The purpose of this document is to provide input to the ICAMSC regarding the use of cloud computing or SaaS technologies in the context of the ICAM segment architecture, specifically as they apply to physical security systems such as Physical Access Control Systems (PACS), video surveillance, visitor management, or any of the related information systems required to fulfill the overall physical security mission of a federal stakeholder.

Specifically, the paper provides the following conclusions:

- SaaS is a valuable implementation technology for multiple ICAM goals;
- A growing number of physical security functions are now available under a SaaS model;
- The SaaS model for delivery of security services offers significant cost and energy efficiencies to the federal IT enterprise.

¹ Federal Chief Information Officer Council, Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance (Washington: US Government, 2009).

FICAM and Physical Security

The Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance is introducing significant changes to the management of three interrelated components of the physical security discipline:

Identity: Whereas physical security systems have long maintained a separate, stove-piped store of the identities needed to control access to property and resources, they must now be federated or synchronized with other identity stores that are used for logical access and other aspects of personnel management. This shift places a renewed emphasis on interoperability and standards, as well as cyber security and privacy.

Observation: Because SaaS centralizes computing resources and provides massive scale, it simplifies the tasks of federation and interoperability by reducing the total number of entities that need to be coordinated. It also places computing resources within secure computing facilities, where PII provisions and other data protection measures are better enforced than in the field.

Credentialing: Whereas physical security systems have long provided native capability for issuing credentials within their own closed population of users, they must now recognize exogenous credentials whose validity derives from independent authorities, such as the federal credentialing process introduced as a result of HSPD 12. Further, these credentials are far more sophisticated than those of the past, featuring such innovations as smart cards, PKI, cryptography, and multiple data fields.

Observation: SaaS systems allow credentials and user management activities to span very large populations, providing coherence across many geographically dispersed sites and facilities.

Access & Authentication: Whereas physical security systems have long managed access privileges and authentication decision on a local, system-by-system, building-by-building basis, this balkanized approach no longer fits the complex needs of our times, and provides inadequate security protections due to the sheer unmanageability of the large, overlapping and often contradictory or outdated data sets spread across the federal physical security enterprise.

Observation: The inherent scale of SaaS systems permit 10's of thousands of buildings and 10's of millions of credentialed personnel to be managed under a single, uniform set of access and authorization policies.

All three of these changes will have widespread—and positive—effects on the physical security industry, as well as challenges for both manufacturers and end users as we jointly discover the best transitional paths to the end state envisioned by the FICAM mission.

SaaS and FICAM

SaaS is directly relevant to the FICAM mission because it promotes efficient implementations of the FICAM segment architecture in furtherance of **ICAM Goal 5**, Reduce Costs and Increase Efficiency Associated with ICAM.

Relevant SaaS characteristics, as enumerated by NIST, that support this goal include:

- on-demand self-service
- broad network access
- resource pooling
- rapid elasticity, and
- measured service

All of these support not only the specific goals of reducing costs and increasing efficiency in the FICAM context, but also the broader federal IT goals of IT modernization, data center consolidation, and increased energy efficiency.

SaaS Maturity and Multi-Tenant Software Architectures

In this context, as an organization that has been providing SaaS service for over eight years, we observe that many of these cost and efficiency benefits are strongly coupled with the “SaaS maturity level” of the applications used within the cloud itself, which is determined by:

- Scalability
- Multi-tenancy
- Configurability via metadata

Of these, multi-tenancy is significant for achieving the cost reductions benefits for new IT systems.

The core idea of multi-tenancy is that “all users and applications share a single, common infrastructure and code base that is centrally maintained”.² Just as a building’s structural architecture will differ depending on whether it is designed for a single occupant or multiple tenants, so too will a software system’s design differ depending on whether it is intended to be used by a single “tenant” or multiple tenants. In this model, cost savings are achieved both through commonality of hardware resources, as well as sharing licensing and operating expenses more efficiently across a large population of users.

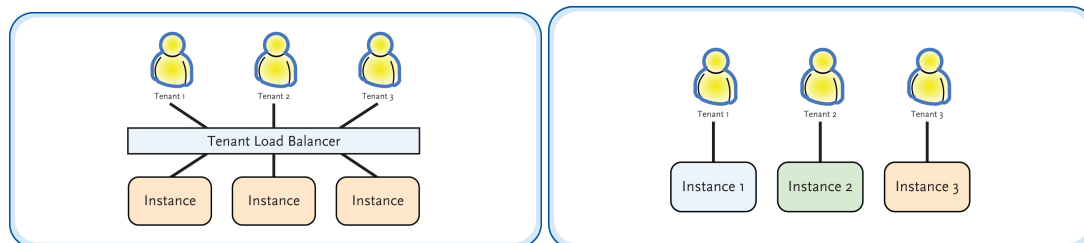


Figure 1. Multi-tenant vs. Single Tenant Software Architecture

² Salesforce.com, "Multi-Tenant Platform," 5 Sep 2009, [salesforce.com](http://www.salesforce.com/au/platform/why-ondemand/multi-tenant-platforms/), 5 Sep 2009
<<http://www.salesforce.com/au/platform/why-ondemand/multi-tenant-platforms/>>.

Multi-tenancy stands in sharp contrast to the practice of simply deploying a stack of client-server systems in a data center and calling it a hosted service. In its “Four Level SaaS Maturity Model,” Microsoft categorizes the multiple server approach as the “lowest level” of SaaS maturity, or roughly equivalent to the “traditional application service provider (ASP) model of software delivery, dating back to the 1990s,” which “offers few of the benefits of a fully mature SaaS solution.”³

SaaS and Physical Access Management

Within the last decade, Web-based application services and metered service business models have established SaaS as the dominant new paradigm for software deployment and delivery. During the same period, the physical security industry matched the broader IT market’s widespread adoption of IP networking technology and ushered in numerous IP-based products of its own, from cameras to control panels to browser-based user interfaces. These two technology trends have converged with the evolution of the service-based economy, in which vendors evolve toward providing higher-value services that free end users from technology management tasks.

Observation: SaaS and related cloud services are now a mature model within the physical security market, with wide commercial adoption across enterprises of significant scale.

The Emergence of Security-as-a-Service

The result of these trends is what many in the industry are now calling *Security-as-a-Service*. Like numerous other application domains, physical security is now moving to the cloud leverage the cost, flexibility, and ease-of-deployment advantages that are cited in numerous industry surveys regarding SaaS adoption drivers.

The general model for Security-as-a-Service is that a technology provider hosts the security management applications on behalf of the end user, and provides them on a metered, pay-as-you-go basis. The end user is generally still responsible for actually administering the contents of the application itself via a browser based interface. In the case of PACS systems, for example, such administration would consist of provisioning permissions for credential-holders, reviewing event history for exceptions, establishing schedules for operating hours of facilities, and so forth.

Relevance of Security-as-a-Service to ICAM Goals

With respect to the goals of ICAM—specifically, **ICAM Initiative 7, Modernize PACS Infrastructure**—the most directly relevant type of Security-as-a-Service is Physical Access Control Systems (PACS). PACS architectures have long been dominated by on-site servers at each federal facility, “creating considerable redundancies and inefficiencies in agency management of ICAM functions.”⁴ With the advent of SaaS, however, there are opportunities for centralization and scaling that were previously unavailable.

Architecturally, SaaS PACS applications use a combination of on-premise embedded hardware modules plus cloud-based applications and data storage. The on-premise equipment is typically the same type of local control hardware that is seen in the current generation of IP-based security equipment: access control panels or edge devices, card and biometric readers, switches, sensors, electric door strikes, and the like. In this context, all of these components connect the local facility back to the SaaS data center in the cloud (public, private, or otherwise, as discussed

³ Microsoft Corporation, "Architecture Strategies for Catching the Long Tail," April 2006, [Microsoft Developer Network](http://msdn.microsoft.com/en-us/library/aa479069.aspx), 1 October 2009 <<http://msdn.microsoft.com/en-us/library/aa479069.aspx>>.

⁴ Federal Chief Information Officer Council, [Federal Identity, Credential, and Access Management \(FICAM\) Roadmap and Implementation Guidance](#), ICAMSC (Washington: US Government, 2009), p 38.

below). The primary efficiency of this approach is to eliminate the server and storage infrastructure at each individual site or tenant space. All PACS applications and data reside in the cloud, at redundant, disaster tolerant data centers, as shown in the diagram below:

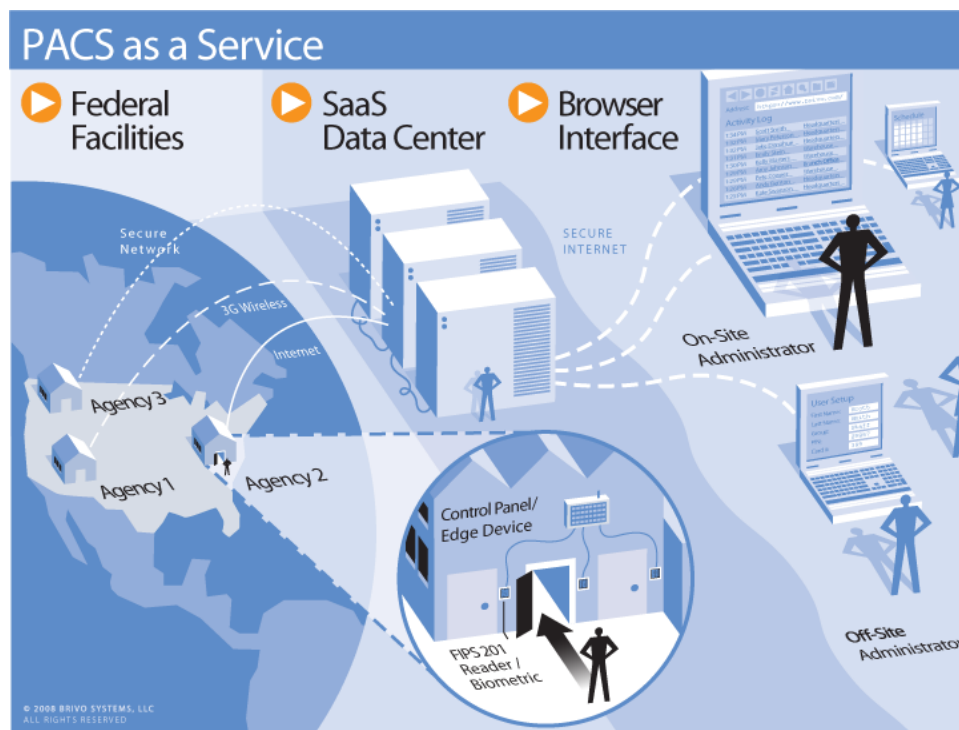


Figure 2, PACS as a Service

Role of Standards

Any discussion of improving enterprise IT efficiency must necessarily address the topic of standards. As the ICAMSC is aware, SIA is an ANSI SDO and has been developing standards for the security industry, collectively known as the Open, System Integration, and Performance Standards (OSIPS). These standards are referenced in Appendix G of the ICAM document. The purpose of the OSIPS standard is to:

- provide a component reference model for the security system of the future;
- provide interface standards to enable interoperability across disparate systems;
- reduce overall cost to end users by promoting compatibility across vendors;
- enable communication with other SDOs to harmonize security industry standards with those of other industry groups.

In the context of cloud computing, all of these goals are still relevant—perhaps even more so as conventions for SaaS applications are still in a formative stage. This situation provides a unique opportunity to drive standardization that is not possible with many of the legacy applications used in security today.

The ICAM document cites four OSIPS standards in particular that are relevant to the ICAM mission.⁵ In creating these standards, it was SIA’s goal to create “bindings-neutral” reference models for the components in a physical security system, the interactions between them, and the types of data they exchange. Bindings-neutral means that the models are abstract in the sense that they do not dictate particular “wire” protocols and data. The reason for this neutrality is that different deployments of equipment and systems may benefit from different bindings to specific transmission protocols and data representations. For example, what is best for high-bandwidth interactions between two security components on a local area network may not be the best for low-bandwidth interactions with devices communicating via a cellular network.

In establishing particular implementations of the OSIPS standards for SaaS or cloud systems in the ICAM framework, there are several conclusions from current best practices in commercial SaaS systems that the ICAMSC should consider as it moves forward.

By their very nature, PACS systems are geographically distributed, and, therefore topologically distributed on the IP networks they use to communicate to other entities in the overall physical security enterprise. This fact suggests several design principles for SaaS-based security systems and the standards used to ensure their interoperability, in furtherance of **ICAM Goal 4**, Enable Trust and Interoperability:

1. Device discovery begins at the edge and moves to the center.

In a geographically distributed enterprise, there is usually a heterogeneous network architecture in which facilities will use different IP service providers, network architectures, firewall policies, and addressing and masking schemes. All of these factors conspire against standard device discovery protocols, which assume a high degree of visibility from the “center” (e.g. server or software stack) outward to all of the devices with which they must communicate. These protocols work fine on local area networks, but are inadequate for wide area networks.

Therefore, in order for a SaaS or cloud deployment to be effective, local security components (e.g., control panels, edge devices, intelligent readers, IP cameras) must be capable of “phoning home” to announce themselves to the centralized administrative software system. This can be accomplished through the use of URLs that are published for various shared services, and then configured into devices when they are installed.

For example, an agency using a SaaS PACS system could establish a single cloud deployment for all administrative software services, and then dictate that all local security components be configured to seek the URL for these services when they are installed.

This is analogous to the means by which OCSP/SCVP and PKI resources are used today; i.e., an agency or other administrative jurisdiction establishes a single authoritative source for certificates, then uses path discovery techniques back to this single source for field devices to ascertain validity.

***Recommendation:** Standards for SaaS or cloud implementations should include protocol bindings that permit the discovery process to operate “from the edge to the center”.*

⁵ Op cit, p. 197.

2. Connection establishment begins at the edge and moves to the center.

Most current physical security systems have been designed on the premise that the central software or server stack is the “master,” and that it should initiate all communications connections with component devices. This is exactly the opposite of the way that SaaS and cloud systems operate.

One of the core principles of SaaS and cloud systems is that they are a discoverable resource that can provide a range of services to any authorized entity. They typically do not initiate service provision themselves because there is seldom a way to know who or what needs to be serviced, or when. The model for SaaS systems is that they accept incoming connection requests, authenticate them, and provide services as authorized or contracted for that entity.

In a heterogeneous wide-area network environment with multiple firewalls and information security policies, the “master connects to device” paradigm of current physical security systems is further challenged by the difficulty and inadvisability of allowing “inbound” firewall traffic at each local facility.

On-premise security system components (e.g., control panels, edge devices, intelligent readers, IP cameras) therefore need to traverse local, on-premise firewalls in the “outbound” direction in order to communicate with SaaS or cloud systems that are centrally deployed. This model not only fits with the way that SaaS systems are designed, but also greatly reduces risk of cyber attack at local facilities by reducing the number of open addresses and ports that must be exposed on the network.

In commercial SaaS system deployed today, for example, local edge devices in PACS systems initiate outbound SSL (or TLS) connections on port 443.

Recommendation: Standards for SaaS or cloud implementations should include protocol bindings that permit connections to cloud resources to be initiated by the security components themselves (rather than vice versa).

3. Security components should have their own PKI credentials

While this may seem an obvious recommendation, most IP-based components in current physical security systems have no form of credential or other method to authenticate their identity to the software systems that manage them. The ICAM roadmap clearly contemplates that devices (as a class of Non Person Entities) may need to have their own credentials, and this is even more important in SaaS architectures in the “edge seeks center” framework of the foregoing two recommendations. The SaaS application stack must have some way of authenticating incoming service requests, and PKI is the only reliable way to do this.

Recommendation: Standards for physical security components needs to include a PKI based model for establishing the authenticity of devices and services, particularly for cloud implementations.

Cloud Security & PII

Information security is usually rated as a top concern among buyers considering SaaS or cloud services. In the commercial sector, this concern is usually based on not being able to verify the information security practices of the service provider. In the context of **ICAM Goal 3**, Improve Security Posture across the Federal Enterprise, we must also consider FISMA and other regulations governing the protection of Personally Identifiable Information (PII).

We believe that centralizing applications and data in the cloud offers an improvement of overall security posture, particularly when these applications are subject to a FISMA C&A requirement. In this regard, Federal CIO Vivek Kundra, observes that "when you look at security, it's easier to secure when you concentrate things than when you distribute them across the government."⁶

To Mr. Kundra's point, today most federal facilities have their own individual PACS systems, with applications, databases, and servers all resident at the facility they protect. The vast majority of these have not gone through a FISMA C&A process, which means that they represent a widespread collection of vulnerabilities of unknown risk level. There is also no uniform standard for how much or which types of PII data are stored in each PACS, which again signifies a widely distributed and unquantifiable vulnerability. What this means for the federal PACS administrator is that the present deployment of individual per-building systems represents a potential leakage of PII as it stands today.

Observation: Centralized SaaS deployments of PACS systems offer an opportunity to improve upon current information security practices because they place the PACS applications and data in a small number secure computing facilities, rather than a large number of potentially unsecured locations scattered around the country.

In particular, the "private" or "community" cloud model offers a path to meeting information security requirements while taking advantage of cloud computing efficiencies. In both of these cases, the applications and infrastructure would be subjected to a FISMA C&A process, and logon access restricted to an approved user population through the use of FIPS 201 credentials.

Total Cost of Ownership

The Total Cost of Ownership (TCO) for PACS systems consists of many contributing factors, from installation and maintenance costs to software and computing expenses, as well as compliance and certification costs. These costs are relevant to **ICAM Goal 5**, Reduce Costs and Increase Efficiency.

Other things being equal, we believe that the costs associated with the procurement and installation of most on-premise, embedded PACS components (i.e., components other than computing systems) is nearly identical in SaaS and non-SaaS system architectures. For example, the cost of equipping an entrance with a card reader, electric door strike, and sensors will be the same whether those devices are being controlled a legacy PACS application or a SaaS data enter.

Observation: There are, however, two aspects of PACS TCO that differ widely between SaaS and non-SaaS deployments; namely, cost of computing infrastructure, and cost of FISMA compliance.

⁶ J. Nicholas Hoover, Federal CIO Scrutinizes Spending And Eyes Cloud Computing, 14 March 2009, 15 March 2010 <<http://www.informationweek.com/news/government/enterprise-architecture/showArticle.jhtml?articleID=215900079>>.

Cost of Computing Infrastructure

The cost efficiencies of cloud computing infrastructure have been widely studied, are well documented, and have been recognized throughout the federal IT community. A recent case in point is the study, “Saving Money Through Cloud Computing,” which details a number of state, local, and federal government case studies in the subject.⁷ These costs savings can all impact **ICAM Goal 5**, Reduce Costs and Increase Efficiency.

Numerous studies have also established that the largest part of application and server ownership costs actually exist in ongoing operational expenses, maintenance, and support agreements. This is particularly true of computing systems that provide infrastructure services such as PACS, because they must meet higher availability requirements than ordinary office equipment.

In the case of PACS systems, we find that for managed tenant property and branch offices, the SaaS model for security management platforms offer cost savings of as much as 76%, due primarily to the economies of scale introduced by hosted application services, as well as reduced up-front costs.⁸

One of the reasons that the SaaS solution is so much less expensive is that it uses none of the on-site servers required for a traditional approach. Note that the traditional server-based system architecture requires computing resources at each location, while the SaaS architecture centralizes this resource, yielding a scalable solution that can be shared across a large number of facilities. The absence of on-site servers eliminates initial purchase costs, maintenance fees, upgrade expenses, and energy consumption.

Observation: There are, however, two aspects of PACS TCO that differ widely between SaaS and non-SaaS deployments; namely, cost of computing infrastructure, and cost of FISMA compliance.

Cost of FISMA Compliance

Now that PACS systems are considered subject to FISMA requirements, the cost of compliance is a significant factor in traditional on-site server deployments. Each site where a server is deployed must undergo its own C&A process at a cost of between \$30,000 and \$70,000, according to federal security experts. When multiplied by the total number of sites subject to **Initiative 7, Modernize PACS Architecture**, the expense clearly runs into the 10’s of millions of dollars.

SaaS PACS architectures offer a dramatic reduction in C&A expenses because once the central SaaS system has been certified, that expense is amortized across all the properties making use of that service.

This “Centralized Certification” is exactly the approach advocated in Vivek Kundra’s recent presentation, “The Economic Gains of Cloud Computing,” presented at the Brookings Institution.⁹ In that presentation, he cites the following “Agency Benefits” to this approach:

- Cost savings through reduced duplication
- Rapid acquisition
- Increased security assurance

⁷ Darrell M. West, "Savings Money through Cloud Computing," Brookings Institution, 2010.

⁸ See: http://www.brivo.com/user_data/white_papers/1263487043_mkt-doc-113-tcowhitepaper.pdf

⁹ Vivek Kundra, “The Economic Gains of Cloud Computing,” PowerPoint Presentation, April 7, 2010

*Observation: With respect to **ICAM Goal 5**, reducing costs, a centralized SaaS approach to PACS deployment offers clear cost and security advantages over the traditional duplication of systems on a building-by-building basis.*

Conclusion

As we discussed at the outset, there are three primary considerations for the use of SaaS technologies to execute the FICAM segment architecture:

- SaaS is a valuable implementation technology for multiple ICAM goals, specifically those related to cost, efficiency, and security.
- A growing number of physical security functions are now available under a SaaS model, the most relevant of these being centralized SaaS PACS deployment.
- The SaaS model for delivery of security services offers significant cost and energy efficiencies to the federal IT enterprise.