Applying OSIPS to ICAM

An Application White Paper

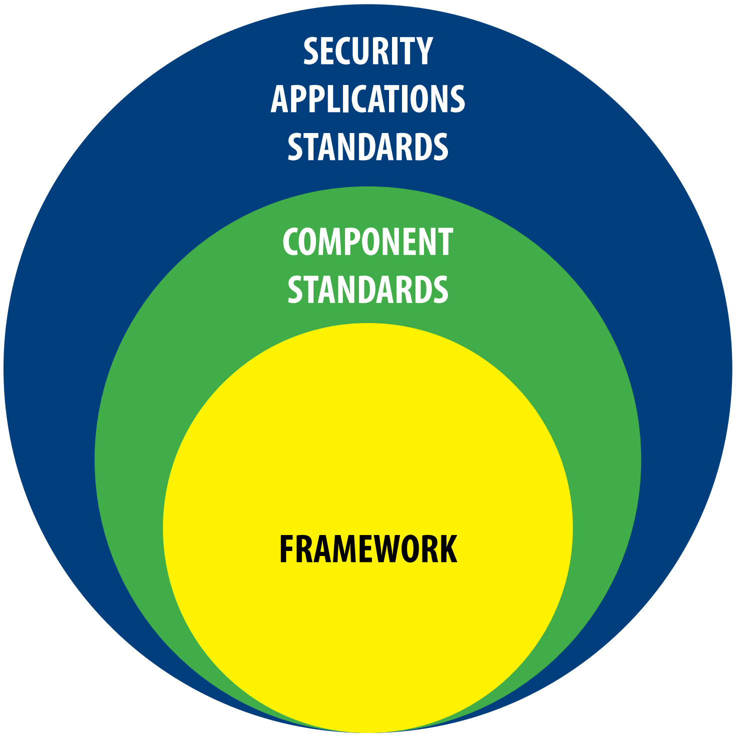
ICAM
Identity, Credentialing,
and Access Management

SIA
SECURITY
INDUSTRY
ASSOCIATION

Executive Summary

The Security Industry Association, an ANSI accredited Standards Development Organization, has a program tasked with the development of open standards for systems integration and performance testing for the security industry. The OSIPS (Open, Systems Integration and Performance Standards) family of standards defines the interfaces to essential components of security systems and this paper outlines how OSIPS may be applied to meet ICAM requirements. These are the type of standards development activities cited in OMB Circular A-119.

OSIPS Reference Model



🔵 **Define the requirements for Security Application Standards**

🟢 **System Component Roles**

- Core Services
- Middleware
- Edge Devices
- Field Devices

🟡 **Foundational / Common Design Elements**

- Event Reporting
- Component Connection
- Capabilities Exchange
- I/O
- Schedules Exchange

As the graphic illustrates, the OSIPS Framework is the core for all OSIPS work. Component standards utilize the framework to enable interoperability. This is then followed by standards for the application of component standards for creating security solutions.

Any enterprise including the government is defined by the aggregation of the systems through which it performs its functions. If the application software of this aggregation fails to operate, integrate or interface effectively, then the enterprise will fail to effectively achieve necessary goals. OSIPS is based on a reference model where systems may be represented as possessing several layers of application software components from core to middleware to edge and field components. A careful analysis of the roles played by each application component is essential to understanding its role within a system. The application components are Core Services, Middleware, Edge Applications and Field Components.

ICAM proposes a vision where these various systems are integrated under an overall operations and analysis application. This application provides for business process policy enforcement, role management, operations audit, compliance reporting, as well as overall monitoring and control of the subsystems of the enterprise. These functions apply constraints on the provisioning of system components to enable comparison of expected versus actual activity. Again, OSIPS standardizes the gathering of information to facilitate these activities. This architecture for the future uses elements of the OSIPS standards to create a Cloud / Software as a Service (SaaS) solution for ICAM that harmonizes access control convergence.

The binding independence of the OSIPS interfaces ensures their applicability regardless of the binding requirements of their deployment environment and consumers. Access control calculation services may be deployed supporting mixed bindings such as SOAP for one collection of consumers, native TCP for another set of consumers, and LDAP for others. Notwithstanding the variations in the wrapper portions of the message, the information content specified by an OSIPS standard will be the same for messages intending the same purpose. Thus, when access privilege calculation is accomplished through the Access Control Role standard, a single instance of a compliant access control role product can support consumers from both the conventional physical access control domain and logical access control domain consumers.

Finally, components require configuration and operational information to successfully function within a system. Provisioning of components includes distributing information while maintaining the consistency of that information throughout the system. Provisioned components:

- understand and engage the environment in which they operate,
- understand the external environment including their provisioners and consumers of their services, and
- have the operating information (dynamic) necessary to perform their functions.

OSIPS interfaces define the messaging for OSIPS components to support integration into systems with proper provisioning that enables efficient transaction processing.

Introduction

Studies by various working groups within Security Industry Association (SIA) Standards have carefully considered established and emerging requirements for U.S. Federal security including those derived from HSPD-12, Federal Information Processing Standard (FIPS) 201, and related Special Publications, other FIPS and related policy efforts. The ICAM Roadmap and Implementation Guidance V1.0 (Part A) is a welcome review of the enormous body of work undertaken over the past several years and lends an important focus on implementation of solutions. With the approval of ICAM Part A and the upcoming publication of Part B, the need for a management level publication relating SIA's Open, Systems Integration, and performance Standards (OSIPS) to ICAM was clear. OSIPS as a family of standards provides the needed references for acquisition of components of near and future ICAM systems and will materially enhance government's ability to minimize risks, costs, and missteps in its work to improve security throughout its enterprises.

OSIPS standards define the interfaces to essential components of security systems. The objectives of this program include:

- Development of standards that define products demanded by a large number of consumers
- Development of standards that are truly open and unbiased toward any product provider
- Development of standards that provide significant and thorough definition of functionality consistent with an overall integrated system reference model capable of defining very large integrated systems
- Develop standards that incorporate testing requirements as needed to establish the compliance of products with the standard.

These are the type of standards development activities envisioned in OMB Circular A-119. This paper demonstrates how OSIPS may be applied for the achievement of the short and long term visions of ICAM Parts A and B. The current published and draft OSIPS standards that are relevant to ICAM include:

Published:

- ANSI/SIA OSIPS-01:2008, Framework
- ANSI/SIA OSIPS DVI-01:2008, Digital Video Interface

Under Development:

- ANSI/SIA OSIPS ACR-01:20xx, Access Control Role
- ANSI/SIA OSIPS APC-01:20xx, Access Point Controller
- ANSI/SIA OSIPS IDM-01:20xx, Identity and Carrier Management
- ANSI/SIA OSIPS ACGO-01:20xx, Access Control Gate Operations
- ANSI/SIA OSIPS DDOV-01:20xx, Design, Deployment and Operation of Video Technology
- ANSI/SIA OSIPS CUIS-01:20xx, Common User Interface Standard

Because OSIPS is a flexible family of standards, the particular approach outlined here may be altered in several ways to accommodate other solutions. This paper should not be confused with an industry position statement. However, the universal applicability of OSIPS enables the definition of multiple system architectures that can meet a variety of security applications and solutions.

ICAM Part A

The ICAM Roadmap provides federal agencies with architecture and implementation guidance that addresses existing ICAM concerns and issues they face daily. In addition to helping agencies meet current gaps, agencies stand to gain significant benefits in security, cost, and interoperability which will have positive impacts beyond an individual agency in improving the delivery of services by the Federal Government. From the access control environment, section 4.7, 4.8, 4.9, and 4.10 of ICAM Part A contain use cases that define expectations for handling access control in a generalized way. This document provides a detailed analysis and reveals details that must be clarified to ensure vital and well performing solutions

Physical access control as a physical security discipline is best defined by its exceptions. Superficially, it is much like logical access control, but, in reality, physical access control practices are laden with essential exceptions that extend the complexity of access control use cases. In particular, the ICAM use cases of section 4.8 and 4.9 are correct yet very basic; actual practices provide a tremendous variety of use case scenarios that specialize these basic behaviors. Most deployed systems incorporate instances of these multiple scenarios that are significant extensions of ICAM 4.8 and 4.9. Logical access control is a relatively less complicated process but does have its own special requirements in practice. Provisioning of access privileges, at a high level, is nearly identical but configuration of physical access points is far more complex due in large part to the diversity of processes and field components associated with access points.

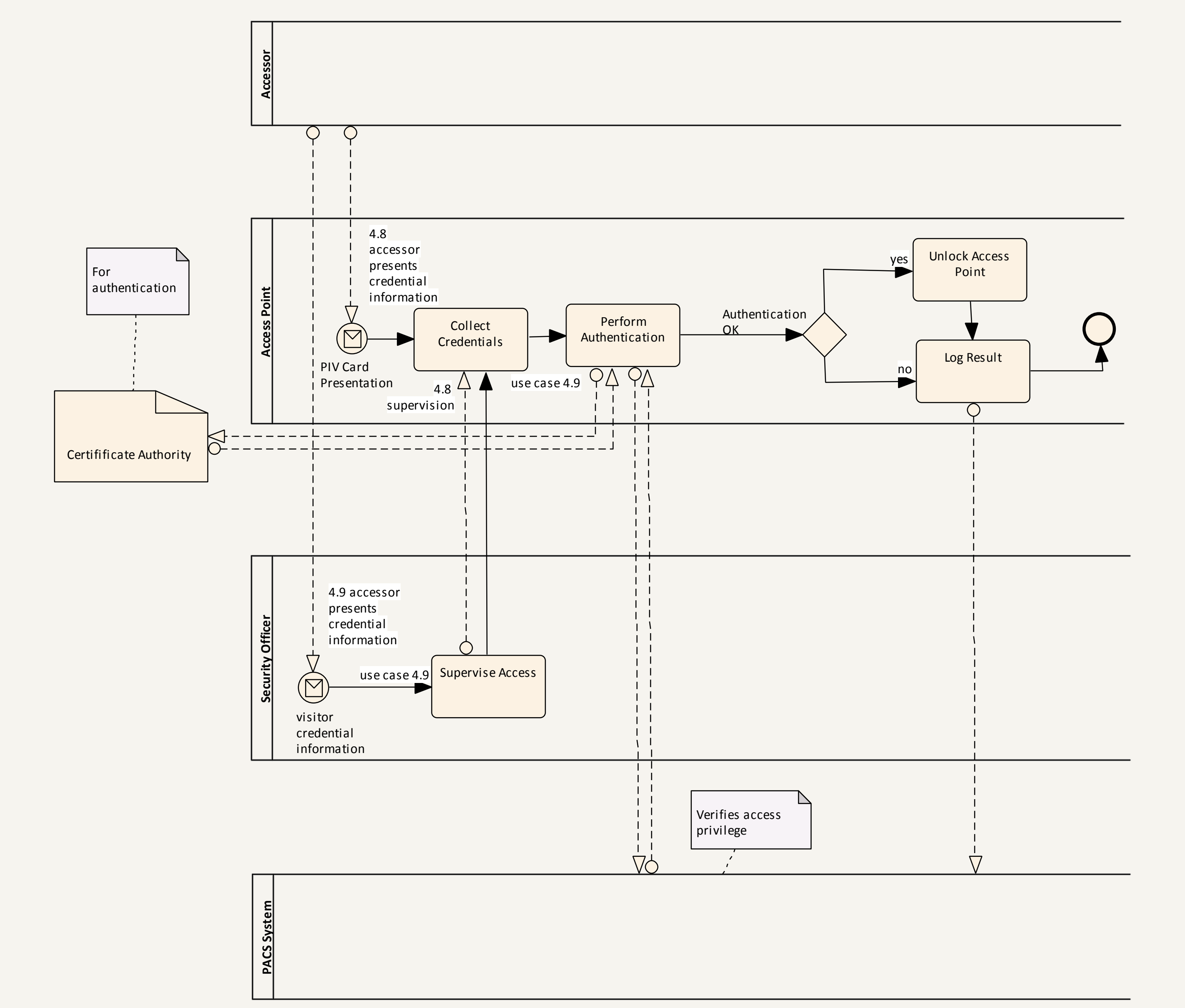


Figure 1: **ICAM 4.8 and 4.9 Basic Use Cases**

For several years now, SIA Standards has been documenting physical access control processes and some logical access control processes along with their many use case scenarios to validate the reference models that support standardization of the processes ubiquitous in both industry and government. Figure 1: ICAM 4.8 and 4.9 Basic Use Cases presents the target state use case 4.8 and 4.9 of Part A as a base reference. The lanes in the diagram depict the key participants of these two use cases. These scenarios incorporate the steps of the use cases documented in sections 4.8 and 4.9 and present graphically the processing flows considered by that document. In this model there are four participants: card holder (Accessor), security officer, PACS, and access point. The Accessor presents the card and credentials in a dialog that, in the case of use case 4.8, are monitored and managed by an access point process with optional supervision by a security officer. Logical access control can utilize the same diagram at this level with the understanding that involvement of a security officer or administrator is very rare.

Logical access has similar issues having to do with the administrative and financial access to systems. Most users are treated in a general way, but exceptions arise involving larger financial transactions, access to private data, and administrative rights to set privileges. Much like physical access, the challenge to define systems lies in the policies for human behavior.

Use case 4.9 is represented in the same diagram with 4.8 to emphasize that the same access point is being operated. The primary distinction between the use cases is in the role of a security officer granting access through an access point. Incorporation of a security officer in the access process is common in physical access control. Typically it is implemented through a long chain of connections involving the PACS and other systems. Several questions need to be answered to define the use case and detail its different scenarios. Some of these questions are:

- What is the mechanism of the security officer’s interaction with the access point and how does the security officer perform the various validations required in their role?
- Is there a graphical user interface (GUI) for the security officer with the access point or is all of the officer’s communications through the PACS or higher central management system?
- Where does the officer get the information needed to perform his or her task?
- Is real time video being utilized?
- What kind of visitor credentials must be assessed and what is the method to validate?

Answers to these questions are essential to the development of a useful implementation guideline. Furthermore, the architecture of different types of access points depends heavily on the answers to such questions.

The practices of ICAM must be appropriate for all access points including access control gates where vehicles including multi-person vehicles and vehicles with cargo must gain entry to a facility. Furthermore, processes where there are more complex rules of access based in part on the state of system elements not directly related to the access point must be considered. Finally, access may be dependent on very specific constraints arising from the number of persons already in a facility, the number of entry attempts, the presence of other individuals of specific types, and a host of other complex rules. ICAM today does not address these potential issues and the traditional approaches seem unlikely to allow the decomposition of the behaviors into well encapsulated activities capable of easy and reliable implementation while meeting all ICAM requirements. However, Part A provides a valuable baseline vision that may be extended by examining practical real world scenarios.

OSIPS Reference Model and OSIPS Standards

OSIPS is founded upon a very flexible reference model. Applying OSIPS to ICAM requires that the ICAM objectives be organized within this reference model. If this is successful then the OSIPS standards are likely to be very useful in meeting ICAM objectives. This section describes the OSIPS Reference Model and the relationship between it and the OSIPS Standards.

Early in the OSIPS effort the need for an effective reference model for security systems was identified because reference models enable the development of many standards in parallel by reducing the risk that work products will conflict or leave gaps. Work toward this model took several years. It was clear that broad industry approval was required if the ensuing technical standards were to be useful. Additionally, the model had to be open-ended so as not to limit future visions of systems capabilities. In 2007, the SIA Standards Roadmap was finalized and approved by the Board of Directors of SIA. While this roadmap is not prescriptive in detail, it provides a basic long term vision that is compatible with possible visions of ICAM’s target endpoint. The OSIPS Reference Model is also compatible with many other disciplines including SCADA, Communications, Fire Alarm, and Emergency Management; plus others not yet established as a part of the ICAM vision.

Adherence to the reference model enables the creation of large scale interoperable solutions. Large scale solutions require operations management and analysis capabilities that will provide line of sight visibility into every component of the system's operation. The delivery of actionable business intelligence to all levels of management without the stakeholder bias of conventional reporting mechanisms enables rapid problem resolution, correction of compliance problems, and continuous improvement of the system's operation.

Any enterprise including the government may be defined by its virtualization in the aggregation of systems that establish its existence. If the application software of this aggregation fails to operate, integrate or interface effectively, then the represented enterprise will fail to effectively achieve necessary goals. Each major system may be represented as possessing several layers of application software components from core components to middleware components to edge components ending with field components. A careful analysis of the roles played by an application component is essential to understanding its role in a system. The application components are:

Core Services Components

The Core Services Component applications of a system are few and provide critical services like central data storage, monitoring, and control over all of the other components of that system. These applications usually operate on powerful servers located at the core of the enterprise's computational infrastructure. These core components will routinely interact with other systems for transaction sharing and exchange of provisioning data while the subordinate components do not interact outside of the system. While the OSIPS reference model fully supports this legacy "stovepipe" view of systems, OSIPS was envisioned with the objective of creating solutions that are interoperable between applications in any layer and any system.

Middleware Application Components

Middleware Application Components typically are deployed on possibly less powerful computers than core services components. They are more frequent within the system architecture and provide distributable points of concentration between core components of any system and the many edge components with which they must interact. In OSIPS, middleware components

- represent core components of any system to distributed collections of edge components (to reduce core component provisioning loads and communications complexity associated with edge component communications and provisioning),
- concentrate communications from collections of edge components to core components (to efficiently use communications resources in edge component to core system component communications),
- provide support for special applications not practical at core components, and
- act as an efficient mechanism for peer-to-peer communications between edge components .

Highly capable middleware components may behave like core components just as simple core components may behave like middleware components to others. It is important to understand the actual roles of these components when developing a solution architecture.

Edge Components

Edge Components house the system's edge application components that monitor and control the actual physical world of the enterprise. There are many, many of these components in a system. This is the system layer that provides the connection between the virtualization of the system and the field components that are a part of the real world and directly sense and control that world. Edge applications reside in edge devices that provide the required, usually specialized, communications ports needed to interact with their field components and the computing hardware and operating system environments needed for the application's operation.

Field Components

Field Components, of which there are thousands in any system, include such things as door sensors, gate operators, signaling lights, locks, temperature sensors, flow meters, intercom and phone stations, card readers, cameras, D/NVRs, and thousands of other devices and instrumentation. Sometimes, depending on system role, specific edge components and field components may conversely actually be field components and edge components.

As the architecture of a particular system is developed, the classification of the role of system components requires thoughtful analysis. It has been shown that selecting components that are manufactured to assume a role inconsistent with the intended role in a design can lead to serious problems in system performance and capability. Within the OSIPS Reference Model, roles for system components have been organized based on real world use cases and experience with real components. It is important to note that any actual manufactured compliant product may incorporate multiple OSIPS standards as the product developer creates solutions for specific market segments.

ICAM Initial System Architecture

The following diagram comes from some recent exchanges discussing ICAM endpoint visions in the near term and in the future. This diagram illustrates a current-technology "stove pipe" approach to achieving policy objectives. The diagram identifies an "Integrator System" that is an essential part of any plan to unify physical security and other enterprise activities in the vision of ICAM.

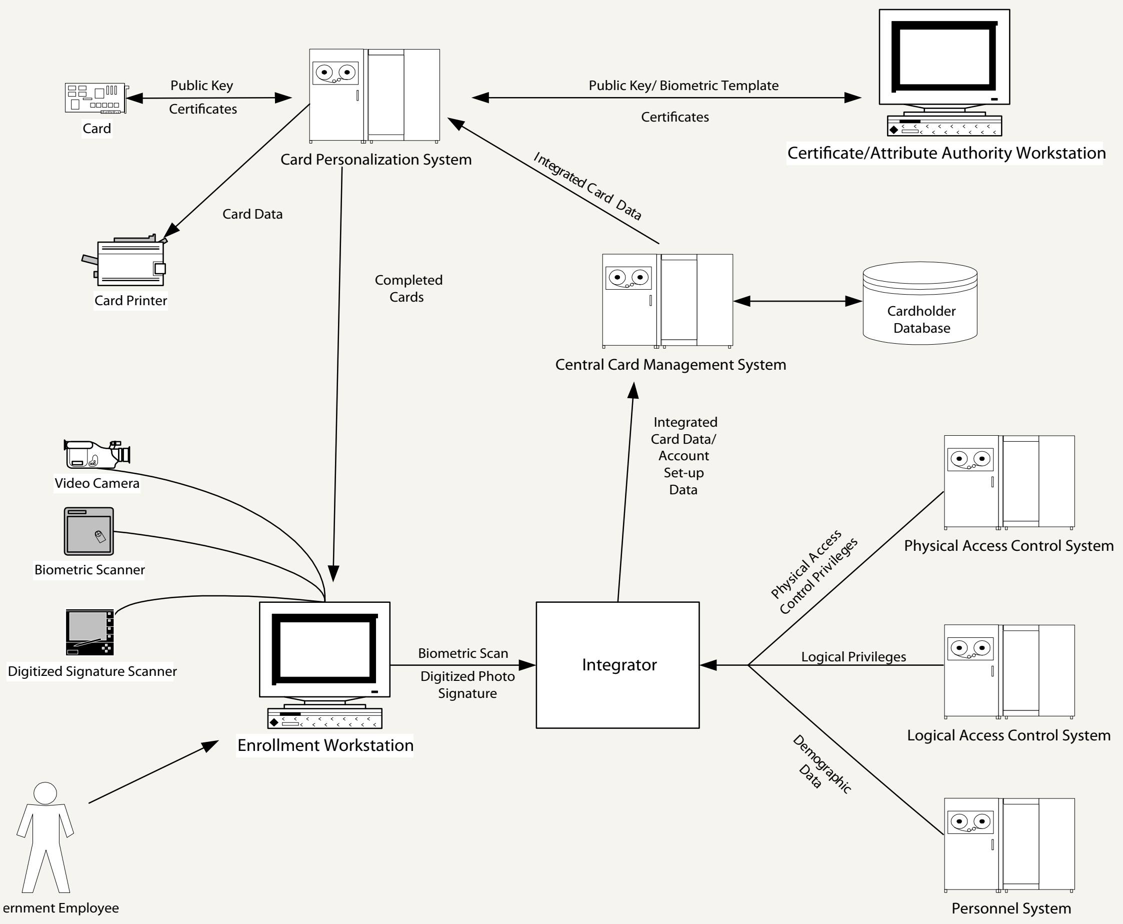


Figure 2: **Smart Card Use Case Concept** [1]

[1] From US Government Smart Card Handbook 2004

Part B discussions suggest a cloud services model as the future endpoint vision for ICAM and the above architecture does not advance that cause except suggesting a central database for all systems. Clearly, unification of the management of the identity, credential validation information, and personnel information across all government facilities is an essential objective in addition to optimizing management and analysis of the entire system. Over time the Integrator will likely evolve to become the operations management and analysis capability.

A LACS administrates local policy for access to local systems, domains, databases, etc. Here 'local' is defined to mean the access points and accessible components under the control of a particular LACS. Policies for access based on accessor roles are administered locally based on rules established by the authority having control over the accessible components. Similarly, a PACS system administrates local policy for access to facilities, perimeters, and areas. Here local is defined to mean the access points and accessible components under the control of a particular PACS. Again, policies for access based on accessor roles are administered locally based on rules established by the authorities having control over the accessible components.

As shown in the 2004 Smart Card use case, centralization and interoperability was envisioned. The 'Centralized Physical Security Information Management (C-PSIM) "integrator" systems of today will interoperate in real-time with various multi-brand, multi-technology based PACS installed in an agency along with LACS to create a unique interoperable bridge between the physical and logical security spaces.

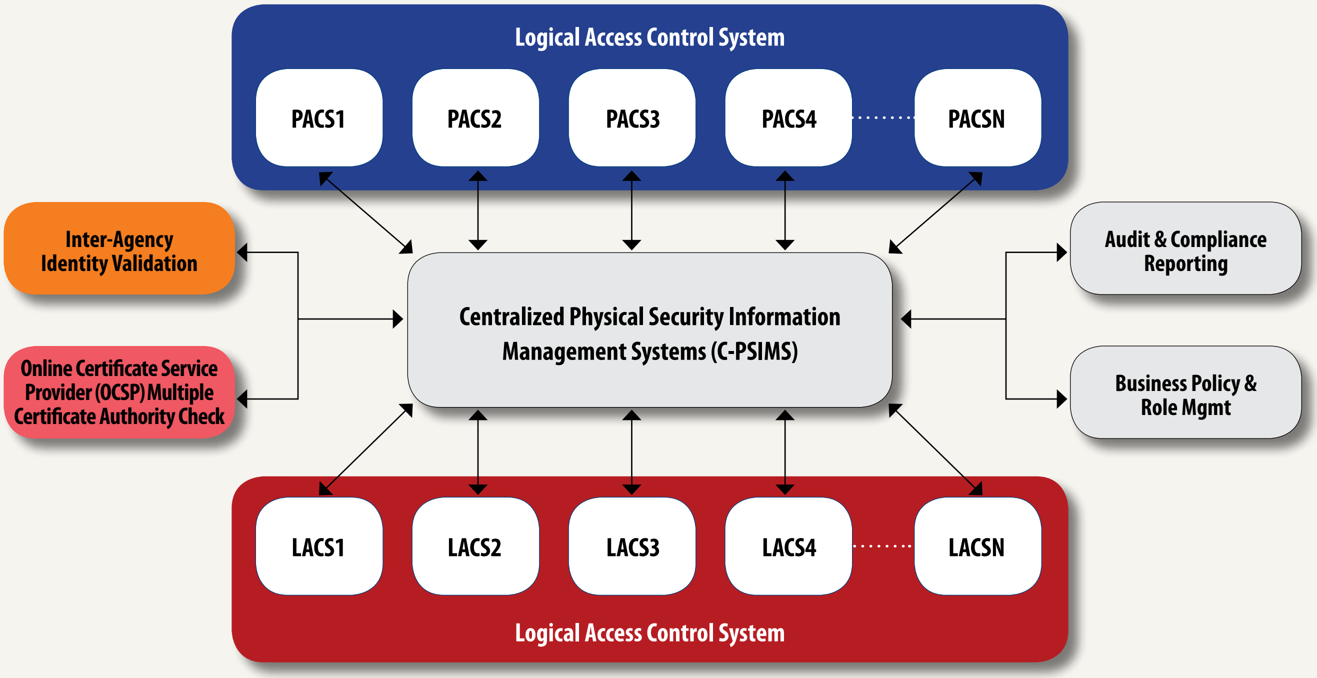

Logical Access Control System
PACS1
PACS2
PACS3
PACS4
PACSN
Inter-Agency Identity Validation
Online Certificate Service Provider (OCSP) Multiple Certificate Authority Check
Centralized Physical Security Information Management Systems (C-PSIMS)
Audit & Compliance Reporting
Business Policy & Role Mgmt
LACS1
LACS2
LACS3
LACS4
LACSN
Logical Access Control System

Figure 3: **Centralized Physical Security Information Management (C-PSIM)**

The Smart Card Handbook states that the he C-PSIM system will enable the interoperability of an assortment of manufacturer's PACS within an agency's facilities as well as other sub systems such as LDAP[2] and various IT IDMSs. Once an assessor's identity is created in any IT/LDAP system – it needs to be cascaded to the PACS systems. The goal is to streamline identities, reduce redundant manual processes and errors associated with PIV card provisioning and PIV cardholder's management.

The C-PSIM system should provide a simple-standard based approach to manage and monitor the data transfer, devices, applications and support for PACS and LACS integration. The C-PSIM system should conform to the NIST SP800-47 guidelines for systems security, interconnectivity and interoperability. Shown in the above graphic is a generic representation of a C-PSIM system. It is in this future instance that the OSIPS capabilities are fully realized.

[2] LDAP Lightweight Directory Access Protocol

ICAM on OSIPS Example Architecture

Figure 4, "ICAM on OSIPS Example Architecture", illustrates a vision of the future where many types of systems are integrated under an "*Enterprise Operations Management and Analysis System*" or EOMAS. 'Business process policy and role management' and 'audit and compliance reporting' are applications that must be a part of ICAM. These functions will apply constraints on the provisioning of OSIPS compliant components that analyze and compare actual activity with these constraints and on the handling of transactions. Again, OSIPS standardizes the gathering of information to facilitate these activities. In the model, the solution component for these services is the EOMAS. The figure illustrates a possible architecture for the future that uses elements of the OSIPS standards to create a Cloud / SaaS solution for ICAM that harmonizes LACS and PACS.

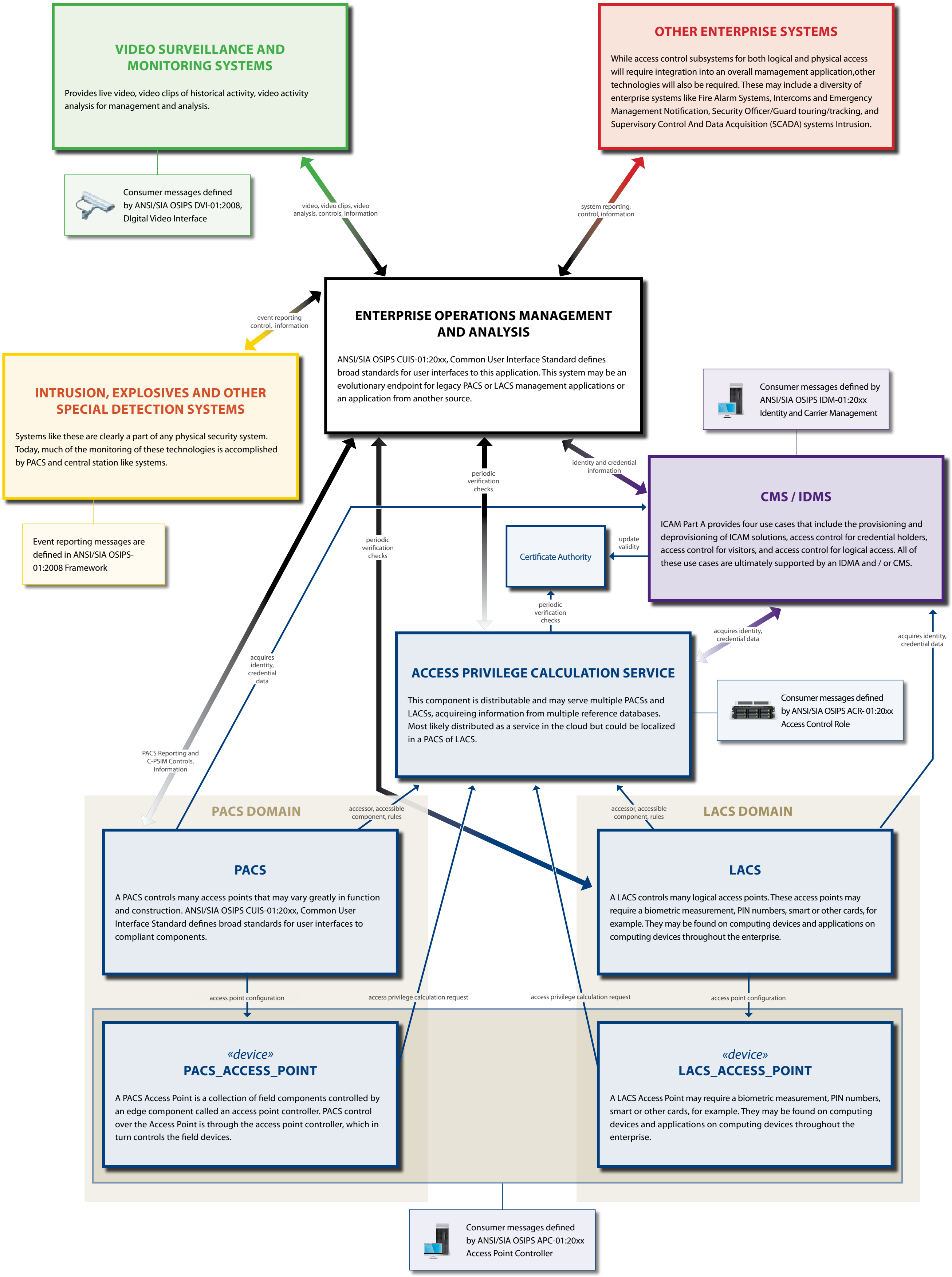
The SIA draft standard ANSI/SIA OSIPS CUIS-01:20xx, Common User Interface Standard defines how information is presented to human users and how they may interact with such systems. PACS, LACS, PSIM, C3, and other 3rd party approaches may evolve to become EOMAS. Note that in most interactions the EOMAS interacts with system components according to OSIPS standards, that is, this system component adapts to the interfaces for the integrated system components. It is anticipated that as this vision is realized, additional standards to regulate presently undefined matters will be identified and created.

A comprehensive security solution requires, at a minimum, real integration of video surveillance and intrusion detection. The published standard ANSI/SIA OSIPS DVI-01:2008, Digital Video Interface specifies the interface of digital video into a system. A portion of ANSI/SIA OSIPS-01:2008 Framework specifies intrusion detection and reporting across all OSIPS Standards. The Framework is an essential component of any family of standards and is discussed below.

In Figure 4 PACS and LACS continue as they do today to provision their respective access points and advise the appropriate access calculation service about accessible components and the identities that have access according to these rules. The access calculation services may support multiple PACS, LACS and CMS / IDMS systems. Video and intrusion detection are integrated at the EOMAS. These elements are explicitly defined by existing OSIPS Standards.

Readers should also note the close association of the physical security access point controller with the logical access point controller. The extent to which these two system components may be harmonized is not presently known, but the business differences between PACS and LACS systems is principally within the edge components and field devices used to request access. Access rules are very similar so consolidating their access calculations into a single service and possibly locating it in the cloud is a solid step towards harmonizing these two very essential components. Such an effort will revise Figure 2, and to some extent redefine the roles of PACS and LACS.

Two general perspectives, transaction processing and component provisioning, are essential to the development of system architecture. Poor design of the locations of information repositories can create tremendous problems for very large deployments. ICAM requirements that include certificate checks, signature validations, and other required trust assurance practices lead to significant transaction loads and great dependency on network availability if these repositories are not properly positioned in the solution architecture. Most practical solutions will dictate repositories must be distributed in such a way that they accomplish the required re-validations and cache the results for subordinate systems.



VIDEO SURVEILLANCE AND MONITORING SYSTEMS

Provides live video, video clips of historical activity, video activity analysis for management and analysis.

Consumer messages defined by ANSI/SIA OSIPS DVI-01:2008, DIgital Video Interface

OTHER ENTERPRISE SYSTEMS

While access control subsystems for both logical and physical access will require integration into an overall mamagement application,other technologies will also be required. These may include a diversity of enterprise systems like Fire Alarm Systems, Intercoms and Emergency Management Notification, Security Officer/Guard touring/tracking, and Supervisory Control And Data Acquisition (SCADA) systems Intrusion.

ENTERPRISE OPERATIONS MANAGEMENT AND ANALYSIS

ANSI/SIA OSIPS CUIS-01:20xx, Common User Interface Standard defines broad standards for user interfaces to this application. This system may be an evolutionary endpoint for legacy PACS or LACS management applications or an application from another source.

INTRUSION, EXPLOSIVES AND OTHER SPECIAL DETECTION SYSTEMS

Systems like these are clearly a part of any physical security system. Today, much of the monitoring of these technologies is accomplished by PACS and central station like systems.

Event reporting messages are defined in ANSI/SIA OSIPS-01:2008 Framework

Consumer messages defined by ANSI/SIA OSIPS IDM-01:20xx Identity and Carrier Management

CMS / IDMS

ICAM Part A provides four use cases that include the provisioning and deprovisioning of ICAM solutions, access control for credential holders, access control for visitors, and access control for logical access. All of these use cases are ultimately supported by an IDMA and / or CMS.

Certificate Authority

ACCESS PRIVILEGE CALCULATION SERVICE

This component is distributable and may serve multiple PACSs and LACSs, acquireing information from multiple reference databases. Most likely distributed as a service in the cloud but could be localized in a PACS of LACS.

Consumer messages defined by ANSI/SIA OSIPS ACR- 01:20xx Access Control Role

PACS DOMAIN

PACS

A PACS controls many access points that may vary greatly in function and construction. ANSI/SIA OSIPS CUIS-01:20xx, Common User Interface Standard defines broad standards for user interfaces to compliant components.

LACS DOMAIN

LACS

A LACS controls many logical access points. These access points may require a biometric measurement, PIN numbers, smart or other cards, for example. They may be found on computing devices and applications on computing devices throughout the enterprise.

«device»
PACS_ACCESS_POINT

A PACS Access Point is a collection of field components controlled by an edge component called an access point controller. PACS control over the Access Point is through the access point controller, which in turn controls the field devices.

«device»
LACS_ACCESS_POINT

A LACS Access Point may require a biometric measurement, PIN numbers, smart or other cards, for example. They may be found on computing devices and applications on computing devices throughout the enterprise.

Consumer messages defined by ANSI/SIA OSIPS APC-01:20xx Access Point Controller

video, video clips, video analysis, controls, information
system reporting, control, information
event reporting control, information
identity and credential information
periodic verification checks
periodic verification checks
update validity
periodic verification checks
acquires identity, credential data
acquires identity, credential data
acquires identity, credential data
PACS Reporting and C-PSIM Controls, Information
accessor, accessible component, rules
accessor, accessible component, rules
access point configuration
access privilege calculation request
access privilege calculation request
access point configuration

Figure 4: **ICAM on OSIPS Example Architecture**

OSIPS FRAMEWORK TECHNICAL SPECIFICATION

OSIPS Framework General Elements

OSIPS Modeling Requirements

OSIPS Common Message Format

OSIPS Framework Common Interface Messages

OSIPS Reference Sequence Diagrams

OSIPS Message Content Structures

OSIPS Special Structures

OSIPS Data Elements Definitions

OSIPS Enumerations and Validation Lists

OSIPS Data Element Type Specifications

OSIPS Conformity Assessment

OSIPS Framework Embedded Models

Component Connection Interface Data Model

Capabilities Exchange Interface Data Model

Event Reporting Interface Data Model

Authentication and Authorization Interface Data Model

IO Point Interface Data Model

Schedules Exchange Interface Data Model

OSIPS Framework Testing

OSIPS Framework Data Element Test Cases

OSIPS Framework Enumeration and Validation List Test Cases

OSIPS Framework Data Type Test Cases

Component Connection Test Cases

Capabilities Exchange Test Cases

Event Reporting Test Cases

Authentication and Authorization Test Cases

IO Point Test Cases

Schedule Exchange Test Cases

Figure 5: **OSIPS Framework Scope**

OSIPS Framework Standard

The charter of the SIA OSIPS activity is to develop standards that enable the easy integration of compliant components into systems. During the development of the early standards, a number of requirements that must be common to all standards were identified. The requirement that OSIPS standards quantify predictable performance led to the requirement that all OSIPS Standards contain a specific plan for testing the compliance of components proposing to be compliant with an OSIPS Standard.

These goals were achieved with the publishing of ANSI/SIA OSIPS-01:2008 Framework. This standard prescribes a family of practices that must be supported by any OSIPS Standard and the shared infrastructure necessary to building an industry wide family of standards. The Framework includes:

As shown in Figure 5, the OSIPS Framework Technical Specification consists of the following:

- OSIPS Framework General Elements – the general elements are the foundational requirements that are used by any interfaces defined in the OSIPS family of standards.
- Embedded Models – the embedded models are those interfaces shared across all components.
- Testing – all OSIPS standards define the testing required to validate a component's compliance.

The OSIPS Framework does not prescribe bindings. The term 'binding' is to be taken as the requirement for application software to associate with appropriate pathways, communications protocols, and message encoding protocols to be able to communicate with other system components. Products that support multiple bindings are ever more important when they are to be used by multiple components and/or systems in multiple disciplines with disparate historical binding preferences. As it turns out, OSIPS supports this condition very well. Without this foundational standard the objectives of the OSIPS Project are obviously unreachable and true interoperability will not be possible.

OSIPS Standards Activities and ICAM Use Cases

During the development of these standards the allocation of function against standards activity was carefully studied from both provisioning and transaction processing perspectives. Standard developers sought to identify appropriate decompositions of the required functionality that create well encapsulated application modules that would permit great scalability, high availability, extensibility, and appropriate distribution.

Transaction processing requirements weigh heavily on reference model architectures. Consider ATM machines or credit/debit card processing terminals. Such systems do not distribute advanced approvals of transactions to all machines since recent activity plays a significant role in the approval of withdrawals or new charges since recent prior activity has an impact on a current transaction request. Establishing a need to synchronize state between thousands of machines is an unrealistic design. Moreover, more sophisticated algorithms that might detect fraud rely on information unavailable to individual machines. In practice, all of the information needed to complete a transaction is collected (the bill is totaled, the card authentication data is collected) and a request for approval is submitted with complete information to permit validation of the authenticity and make an approval. An authorization code or denial is the response. At any access point in any system the business requirements of the access transaction at the point determine the acceptable service times for access. The cost of an ATM-like approach in access control is the incremental increase in time required to secure the remote approval, which is usually manageable or avoided by good planning. Additionally, the availability of the access calculation capability given the probability of communications failures in the context of large systems indicated the need for a middleware access privilege calculation service (interface defined by ANSI/SIA OSIPS ACR-01:20xx Access Control Role) that can be distributed to serve multiple access points on a regional or location basis.

OSIPS Transaction Perspective

Figure 6, "SIA Standards Access Transaction Diagram" represents an access transaction using OSIPS. The Access Point Controller has evolved to be the module that interconnects all access point field components. The great diversty of the devices matches the diversity of access points. The concept of the edge component Access Point Controller provides for access point to access point independence and variability since the instances at different access points can vary greatly.

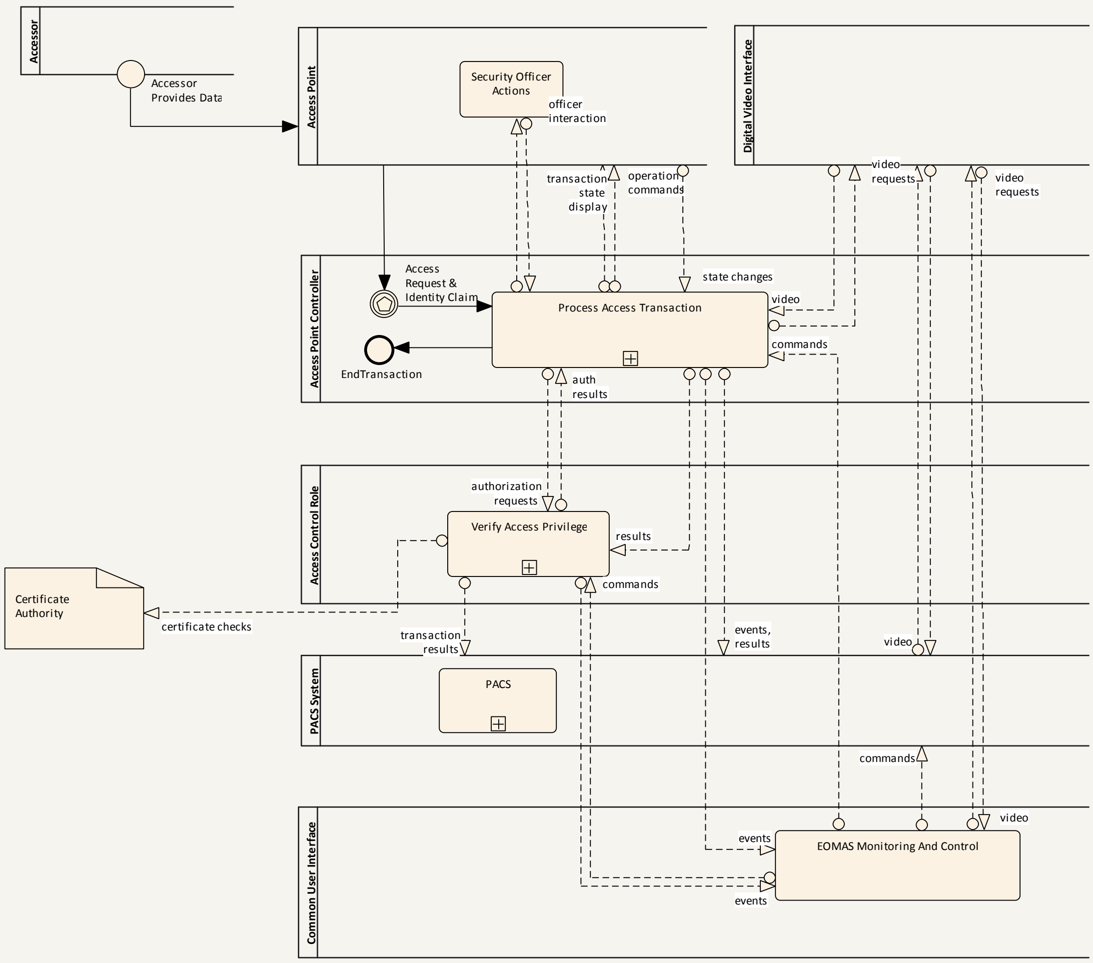


Figure 6: **SIA Standards Access Transaction Diagram**

The Access Control Role has evolved to be a distributable engine for calculation of access privilege where the computation used may vary by access point. This ability to serve many different access points is an important capability in enterprise applications. Using these definitions much simplification of the access control process has been possible. As before, the accessor presents data to devices of the access point, these devices then present this information to the Access Point Controller. It is the Access Point Controller that manages the access point and the process of seeking approval of access for the accessor. This change enables the inclusion of any type of access point under the standard; an essential objective of this effort. Note that the security officer is a part of the access point.

The devices of the access point provide multiple elements of information to the Access Point Controller, which collects information prior to initiating an access decision process. The Access Point Controller determines the sufficiency of information provided to support the access calculation for which it is configured. Not shown in the diagram, a transaction will be abandoned according to various rules should insufficient information be collected. Once the required information is available the access transaction is processed.

After all requisite information is collected it is forwarded as a request for access privilege calculation to the Access Control Role in a like manner to the example ATM transaction discussed above. Current use cases suggest that the "panel" or the Access Point Controller may need to be provisioned with a variety of public key and other data to facilitate the secure collection of required information. This provisioning may have an impact on performance.

The binding independence of these models ensures their applicability no matter the binding requirements of their environment. The access control role may be deployed supporting mixed bindings such as SOAP for one collection of consumers, native TCP for some consumers, and LDAP for others. Notwithstanding the variations in the wrapper portions of the message, the information content specified by an OSIPS standard will be the same for messages intending the same purpose. Thus, when access privilege calculation is accomplished through the Access Control Role, a single instance of a compliant access control role product can support consumers from the conventional physical access control domain and logical access control domain consumers. In fact, this harmonization enables a much more powerful sharing of accessor and accessed components state information thus improving the overall system solution as envisioned in ICAM.

The Access Control Role provides the service of calculating access privilege. An essential observation is the independence of this component. It need not be limited to supporting access for a single PACS. Under OSIPS, it is capable of serving several PACS as well as a diversity of Identity and Credential Database(s). No constraints have been placed on the number and character of provisioners of the Access Control Role or of the system components that provide data to them. A PACS system may provision this module for the access points under its jurisdiction or control. EOMAS and PACS systems will receive reports of access and non-access according to the access points for which it is responsible. These messages are represented in the above Figure 6.

OSIPS Provisioning Perspective

Provisioning refers to the process through which an application component receives the information that allows it to operate according to its designers and owners purpose. Provisioning information includes the information needed by an application to

- understand and engage the environment in which it operates,
- understand the environment external to its operating environment (provisioners, monitoring services and, as in access point controllers, the locks, door sensors, credential readers, and other controlled field components),and
- perform its functions (carrier and identity information, accessible components, and access privileges in the case of a process that provides the service of calculating access privileges).

Provisioning occurs by several means including direct adjustments of configuration files and the operating environment of the application typically by the installers. Provisioning may also include direct interaction through a user interface that supports collection of the information content of the application component, and through interaction with databases that contain information needed by the application component. In this last case the application component may request information or be a recipient of information according to the application component's design.

OSIPS Standards anticipate that application components will have multiple provisioners and, except for the provisioning associated with installation, provides specifications for all types of messaging needed to achieve the level of functionality envisioned by the developers of the standard.

Those familiar with pictures of very early telephone system transmission cables will remember thousands of wires from switchboard locations to individual telephones. Replicating this approach by having each edge component contact one or more database and monitoring service in modern standards is possible. For some system components this might not be a significant problem if the amount provisioning information exchanged was small and very static. But where large quantities of dynamic data are involved such an approach would be impractical. In part, it was the consideration of the provisioning requirements of the many use case scenarios of access control that ultimately led to the consolidation of access privilege calculation information into the Access Control Role standard. A corollary was the allocation of credential gathering and access point operation in the Access Point Controller standard. This division of scope has important impact on the transaction handling characteristics of components realizing these standards, which will be reviewed below. However, it must again be noted that the OSIPS standards define the interfaces of compliant components but they do not limit the construction of real products that might support more than one standard and in some cases some product developers may produce components that support multiple OSIPS interfaces.

Figure 7, "APC / ACR Provisioning In OSIPS" provides a view of the overall provisioning process. When a PACS provisioner updates the Access Point Controllers of a PACS for the purpose of adding, deleting, or updating the properties of its access points, the PACS processes the transaction and updated the Access Point Controller according to its interface. For Access Point Controllers, this information might include access policy at the access point, access point component awareness, configuration parameters, and related elements.

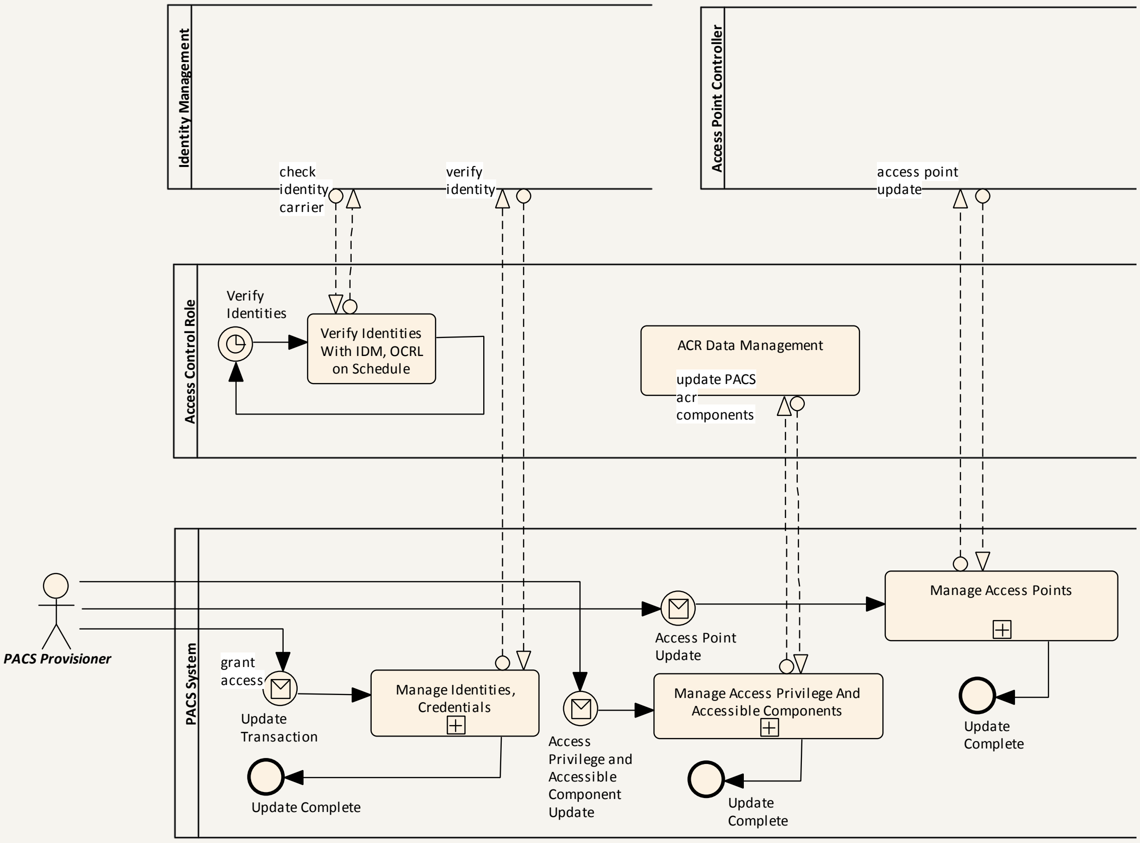


Figure 7: **APC / ACR Provisioning In OSIPS**

When a PACS provisioner adds an accessor, the identity is appropriately verified by contact with the IDMS / CMS containing the individual and any certificate authority needed to ascertain the currency of credentials. The accessor is then entered into the PACS. Subsequently when a PACS provisioner desires to grant access to this accessor, the PACS implements that action by sending update transactions granting access to the appropriate access calculation service. It may be that through a very similar process the PACS provisioner will create a new definition of an accessible component that will be added to an access calculation service.

It must be noted that there is no prescription or suggestion of the type and style of any hardware component in this model. The decomposition is based solely on the participation of the functional components in the process. Realizations of these capabilities will take many forms.

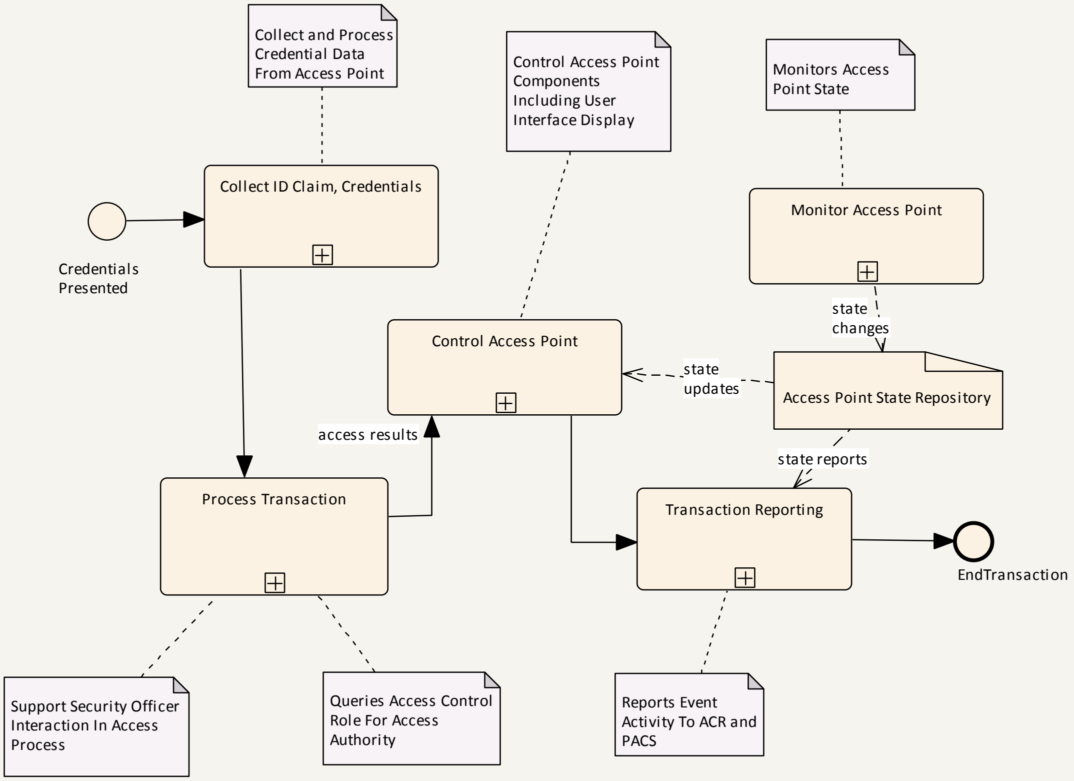

Collect and Process Credential Data From Access Point
Control Access Point Components Including User Interface Display
Monitors Access Point State
Collect ID Claim, Credentials
Credentials Presented
Monitor Access Point
state changes
Control Access Point
state updates
Access Point State Repository
access results
state reports
Process Transaction
Transaction Reporting
EndTransaction
Support Security Officer Interaction In Access Process
Queries Access Control Role For Access Authority
Reports Event Activity To ACR and PACS

Figure 8: **A More Detailed View of the Access Point Controller Behaviors**

Access Point Controller (ANSI/SIA OSIPS APC-01:20xx)

In Figure 8, "A More Detailed View of the Access Point Controller Behaviors", provides a more detailed analysis of the behavior of the access point controller as defined by the draft standard. This discussion is not meant to provide a specification for construction of such a component. It merely serves to illustrate the generally required behaviors of such component acting as a part of a complete system.

Links to external components have been suppressed and are recognized by notes indicating the nature of the information exchanged by those links. This illustrates the basic case for an access transaction in a way that harmonizes ICAM 4.8 and 4.9. Note that we have suppressed provisioning in this diagram. Generally, the PACS that owns an Access Point Controller and the Access Control Role instance that provides access privilege verification provision any Access Point Controller.

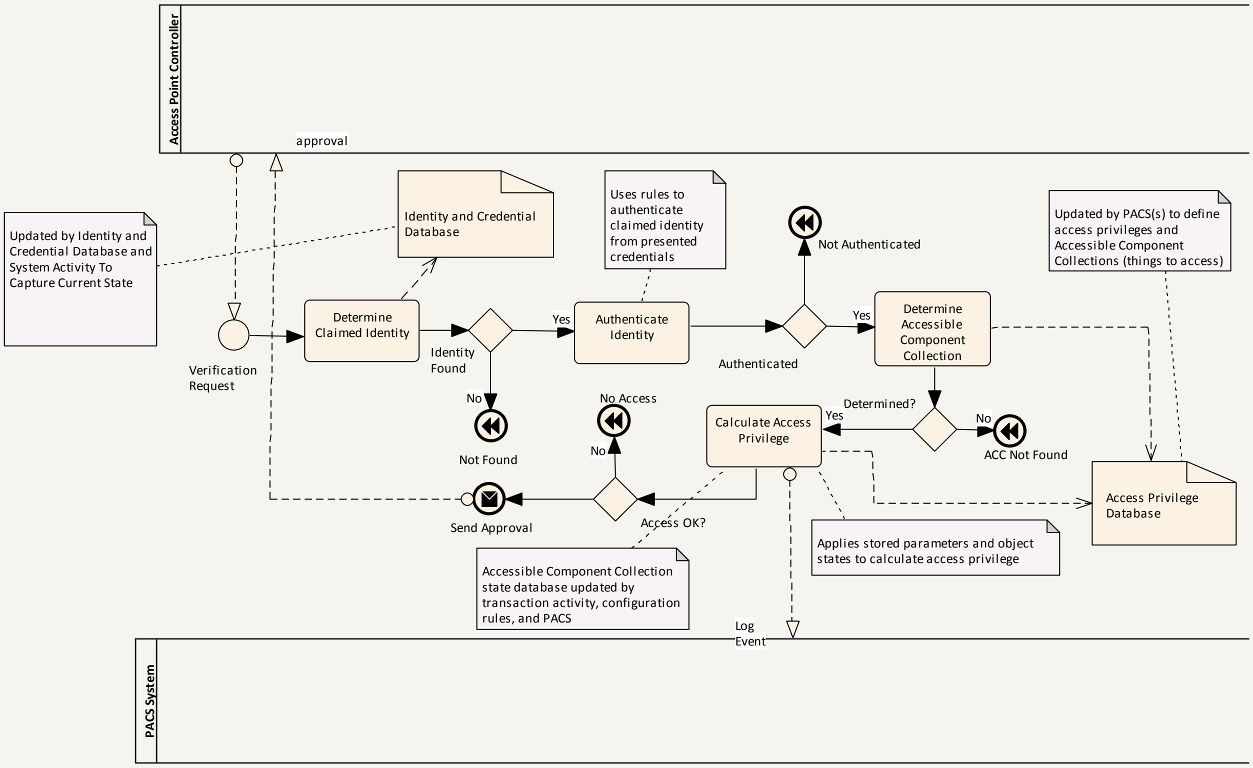
From a base use case perspective, credentials are collected and pre-processed so that an access authorization query may be sent to the Access Control Role. The level of provisioning required of an APC should be studied with an objective of limiting this requirement. It may turn out that provisioning of public keys at the APC is essential and this may be accomplished through the provisioning transactions not shown. The security officer that is an integral part of the access process may interact directly with the APC or, that interaction may be through another system component. Generally, a desire for high availability will recommend a local interaction either through a button of a more sophisticated interface. Most instances of Access Point Controllers will operate autonomously without interaction from a security officer. Note that not all message paths are shown in this high level example.

The Access Control Role calculates access and directs a response to the Access Point Controller activity. It is important to provide local feedback to the accessor, lock and unlock the access point, and be aware of the success or failure of an approved access transaction. This result must be presented to the Access Control Role and to the owning PACS. This information along with pre-programmed changes in access point state is an essential component of the information used to deliver quality access control. These requirements are not articulated in the ICAM document.

Finally, this model is wholly accepting of the diverse sets of technologies that make up access points today. From vehicular access to count controlled access to many others special behaviors and ending in very basic access, system designers and users depend on their systems to manage complex processes. The Access Point Controller (ANSI/SIA OSIPS APC-01:20xx) standard presents a well organized analysis and reference model for these activities. It is a mature model soon to be available as an ANSI standard.

Access Calculation Service and Access Control Role (ANSI/SIA OSIPS ACR-01:20xx)
This draft standard is a comprehensive compilation of the diverse practices used to control access at all manner of access points, physical and logical, including the most complex and frequently some of the most critical for a facility.

Figure 9, "Verify Access Privilege with the Access Calculation Service", summarizes the most simplified successful scenario of a basic access transaction where messaging is defined by the Access Control Role standard. This diagram oversimplifies the process while illustrating the basic steps. An explanation of the complexity of the real-world required access policies exceed the limits of this paper. As an effort to illustrate these complexities, we provide several examples.



Access Point Controller
approval
Identity and Credential Database
Uses rules to authenticate claimed identity from presented credentials
Not Authenticated
Updated by PACS(s) to define access privileges and Accessible Component Collections (things to access)
Updated by Identity and Credential Database and System Activity To Capture Current State
Determine Claimed Identity
Yes
Authenticate Identity
Yes
Determine Accessible Component Collection
Identity Found
Authenticated
Verification Request
No
No Access
Determined?
Calculate Access Privilege
Yes
No
Not Found
No
ACC Not Found
Access Privilege Database
Send Approval
Access OK?
Applies stored parameters and object states to calculate access privilege
Accessible Component Collection state database updated by transaction activity, configuration rules, and PACS
Log Event
PACS System

Figure 9: **Verify Access Privilege with the Access Calculation Service**

Vehicular Access (ANSI/SIA OSIPS ACGO-01:20xx)
While identity verification of the driver is a part of this process, validation of the vehicle and its privilege of access, verification of the association between the driver and the vehicle, status checks about the worthiness of the vehicle, identity verification and access privilege determination for passengers, recording of entries including video records of entry and security officer inspection results are critical to this process. Perimeters are the first line of protection. Preventing a car load of explosives from entering a facility is an essential mission. This very complex example points to the need for much more diverse technology deployed at vehicular gates and much more significant validation reference data at an ACR than those contemplated by ICAM.

Controlled Count Example
In this example an area within a facility is subject to rules of access that apply special constraints like minimum and maximum numbers of accessors within the area, the presence of supervisors in addition to regular accessors including the maintenance of a ratio between these subgroups, and conditions on the state of the facility, which may be complex. Typically, the most critical facilities have the most complex rules. The problem is complicated by the typical use of several access points in the operation of this area.

These two common examples illustrate the typical complexity of access control at secure facilities. Figure 9 illustrates how a transaction might traverse the access calculation service and how information resources may be applied to the calculation of access.

The developers of this standard have studied many examples in its development. An instance of the access control role might be placed at any location(s) within the enterprise solution, and some will want to place it in the same hardware environment as the access point controller. The standard takes no position on such decisions, but it should be noted that provisioning such a component is a significant task especially in an environment requiring continuous re-verification of the authenticity of credentials. A reasonable designer will encapsulate solution components in the most efficient manner to achieve mission requirements. The Access Control Role (ANSI/SIA OSIPS ACR-01:20xx) standard presents a well organized analysis and reference model for these activities. It is a mature model soon to be available as an ANSI standard.

Standards Activities Overview

ANSI/SIA OSIPS-01:2008, Framework

This standard prescribes a family of practices that must be supported by any OSIPS Standard and the shared infrastructure necessary to building an industry wide family of standards. The OSIPS Framework defines a set of common design elements required including interfaces for security component connections, capabilities exchange, event reporting, I/O (input/output) and schedules exchange. The requirements for testing as well as tests scripts for each embedded interface are defined.

ANSI/SIA OSIPS DVI-01:2008, Digital Video Interface

For video surveillance and monitoring systems, this standard defines an interface for the control of live and recorded video as well as camera control. It provides for the reporting of events and status including position, direction, speed and other complex video analytic events.

ANSI/SIA OSIPS ACR-01:20xx, Access Control Role

This standard defines the interface to an access calculation service for access control as a role-based application unifying traditional (physical) and IT (logical) access control.

ANSI/SIA OSIPS APC-01:20xx, Access Point Controller

This standard defines an interface to an access point controller that manages the access point and the process of seeking approval of access.

ANSI/SIA OSIPS IDM-01:20xx, Identity and Carrier Management

This standard defines interfaces for systems that manage personal identity, carriers, containers and credentials.

ANSI/SIA OSIPS ACGO-01:20xx, Access Control Gate Operations

This standard defines an application role that integrates a variety of components based on the scale and diversity of requirements for access control of gate operations. Specific instances of the application provide individual, vehicle and cargo verification, access control services, gate surveillance, intrusion detection and other services.

ANSI/SIA OSIPS DDOV-01:20xx, Design, Deployment and Operation of Video Technology

This standard defines the criteria for the selection of video technological capabilities based on application requirements, the deployment of such technology including its integration, and the operation of the deployed system.

ANSI/SIA OSIPS CUIS-01:20xx, Common User Interface Standard

This standard defines the criteria for user interface components in the operation of systems that provide command, control, communications and related services for operating personnel.

Security Industry Association
Information. Insight. Influence. www.siaonline.org