SETECS
Secure Transactions and Electronic Commerce Systems

Tel: 240-535-2095 **http://**security.setecs.com **E-mail:** sead.muftic@setecs.com

SETECS® Security Technologies

Concept, Design and Current Implementation of the Comprehensive Security System for Cloud Environments and Applications

White Paper – July 20, 2013

Executive Summary

Cloud computing is becoming more and more popular computing paradigm. Using remotely hosted applications and on–demand, with even all user resources stored at remote servers ("virtual servers") has many advantages compared to the standard, client–server environment.

However, in such environments, security has much more important role than in classical network, client–server, environments. Not only that the same, standard, security services are needed (authentication, authorization, confidentially, integrity, authorization, etc.), but their provision must be offered to clients transparently and in an environment comprising distributed components and delegated authorities. Cloud computing makes security not only much more important, but also much more difficult to organize and manage, due to the transparent nature of cloud resources, components, and services.

In this white paper we describe the details of the concept, design and current implementation of the comprehensive security system for cloud environments and applications. The system is compliant with Government FICAM initiative (Federated Identities, Credentials, and Access Management), it can perform all its thirteen use cases (FedRAMP Roadmap), and performs its security services fully compliant to the FedRAMP baseline security controls. The system has six groups of components and provides six groups of services:

Identity Management System (IDMS) which registers all components and participants in cloud–based applications and provides reliable source of their identities.
Public–Key Infrastructure components and services, comprising four Certificate Authority (CA) Servers organized in a hierarchy and supporting all certificates and CRL protocols.
PIV Card Management System, with all its components and stations, as required by the FIPS 201 standard: Sponsor Station, Enrollment Station, Issuing Station, Card Management Station, and Card Management Server.
Strong Authentication Server, Client and Protocol based on FIPS 196 standard, using two–factor authentication based on PIV cards. The system supports single sign–on protocol based on SAML standard.
Role–based Access Control System compliant to XACML standard with flexible Policy Administration, Policy Decision and Policy Enforcement components.
Cloud/Portal Secure Gateway, the component that provides security to Web Portals, Cloud Platforms and Virtual Servers in a cloud environment.

The system is fully functional and based on shared service providers. It is easy to install, configure, activate and deploy.

1. Introduction: Security Requirements – FICAM Use Cases

The requirements for a comprehensive security system and at the same time features of the SETECS® Cloud Security System can best be specified by quoting the roadmap for FICAM activities in individual Government agencies and even commercial enterprises (Federal Identity, Credential, and Access Management (FIAM) Roadmap and Implementation Guidance"). The document specifies thirteen use cases for the comprehensive security system, as follows:

1.1 Create and Maintain Digital Identity Record for Internal Users

This use case provides the high-level process steps for establishing a digital identity for an internal user and modifying the digital identity record over time as the user's attributes change. This use case is distinct from credentialing (covered in Use Cases 1.4, 1.5, and 1.6) in that identity records can be created without the issuance of a credential.

1.2 Create and Maintain Digital Identity Record for External Users

This use case provides the high-level process steps for establishing a digital identity for an external user and modifying the digital identity record over time as the user's attributes change. This use case represents a complex and varied set of mission-specific scenarios through which federal agencies collect and maintain personal information for users external to their agencies

1.3 Perform Background Investigation for Federal Applicant

This use case provides the high-level process steps for conducting a background investigation for a federal employee, contractor, or affiliate. The background investigation often results in a determination of suitability/fitness for federal employment or fitness to perform work as a contractor.

1.4 Create, Issue and Maintain PIV Card

This use case provides the high-level process steps for creating and issuing a PIV credential to a federal employee or contractor, as defined by FIPS 201. This use case also provides the high-level process steps for maintaining a PIV card over the life cycle of the card.

1.5 Create, Issue and Maintain PKI Certificate

This use case provides the high-level process steps associated with creating, issuing, and maintaining a PKI certificate over the credential life cycle in compliance with Federal PKI standards. PKI certificates can be issued as software, or soft certificates, where the private key of the PKI key pair is installed as part of a software application, usually directly to a computer or other devices. Alternatively, PKI certificates can be issued as hardware certificates, where the private key is installed on a protected hardware token that has been tested and certified to be FIPS 140 compliant.

1.6 Create, Issue and Maintain Password Token

This use case provides the high-level process steps associated with creating and issuing a password token to a user and the maintenance steps required to change the password at periodic intervals or when it has been forgotten or compromised. Password tokens are typically created specifically by and for the application being accessed and the process is often closely tied to creation of a digital identity record and user account within the application.

1.7 Provision and De-provision User Account for an Application

This use case provides the high-level process steps for provisioning and de-provisioning a user account in an agency application. It includes the creation and subsequent removal of a user account and the assignment and management of the appropriate privilege (or entitlement) attributes for access to applications and other resources.

1.8 Grant Physical Access to An Employee or A Contractor

This use case provides the high-level process steps for granting routine physical access to a facility or site to internal agency employees, contractors, and affiliates who require PIV cards.

1.9 Grant Visitor or Local Access to Federally Controlled Facility or Site

This use case provides the high-level process steps necessary to authenticate and authorize a visitor or an individual who requires local physical access to federally-controlled facilities and sites. A visitor is an individual external to the agency who requires access (often short-term or intermittent) to a facility or site controlled by the agency. Local access or facility access applies to an individual who requires more long-term access, typically to a single facility, but who does not qualify to receive a PIV card.

1.10 Grant Logical Access

This use case provides the high-level process steps for authenticating and authorizing a user to grant logical access to systems, applications, and data. The use case applies to both internal and external users using government and commercially-issued credentials to gain logical access across all assurance levels.

1.11 Secure Documents or Communication using PKI Credentials

This use case provides the high-level process steps for digitally signing or encrypting data and electronic communications using the most common system tools available within the Federal Government. Encryption is the process of transforming data from a readable form into a form that requires an individual to possess a cryptographic key in order to read it. It is used to provide confidentiality for data.

2. SETECS® ICAM System – Components and Architecture

SETECS® Cloud Security System provides all the functions listed as requirements in the previous section. Individual requirements or groups of them are supported by individual subsystems, while the components and subsystems are at the same time mutually integrated to provide fully federated architecture.

2.1 Components – Subsystems

SETECS® ICAM system comprises six components that can be considered as subsystems of the system. Each of these components provides one group of specific security functions, while collectively they provide a comprehensive set of security services.

Identity Management System (IDMS) registers all components and participants in cloud–based applications and provides reliable source of their identities. Registration attributes used by the system are compliant to the Simple Cloud Identity Management (SCIM) system. Its functions and services are compliant with FedRAMP baseline security controls.

Public–Key Infrastructure system components are four Certificate Authority (CA) Servers organized in a hierarchy: Top (Root) CA Server, Policy CA Server, Geo–Political or Organizational CA Server and Issuing CA Server. The system supports all certificates and CRL protocols: receiving requests, issuing certificates and CRLs, distributing them to users and Relying Parties, and verification of certificates.

PIV Card Management System has all components as required by the FIPS 201 standard: Sponsor Station, Enrollment Station, Issuing Station, Card Management Station, and Card Management Server. The system can register applicants, enroll them, issue them PIV card, activate the card and maintain PIV cards after their issuance.

Strong Authentication System provides strong authentication protocol, based on challenge/response in accordance with FIP 196 standard. In addition, the system provides single sign–on protocol based on SAML standard. Both protocols support three–factor authentication based on PIV cards (PIV card, PIN and PIV Authentication Certificate).

Role–based Access Control System enforces authorizations to access and use applications and their resources based on user roles. It is compliant to the XACML standard. The components of this

subsystem are Policy Administration Interface, Policy Decision Server and Policy Enforcement Server.

Cloud/Portal Secure Gateway is the component that supports security to Web Portals, Cloud Platforms and Virtual Servers in a cloud environment. It provides authentication of users by verifying their identities, their authorization to perform certain requests, and protection of data and messages being communicated between users and Application Portals.

2.2 System Architecture – Shared Security Servers

The architecture of the SETECS® ICAM system is in the form of shared security servers. IDMS, PKI, PIV, Strong Authentication and Policy Decision subsystems are grouped in the form of an integrated server that can be shared by multiple Replying Parties. Relying Parties are stand–alone Web Portals, cloud platforms, or individual Virtual Servers located in the cloud virtualization environment.

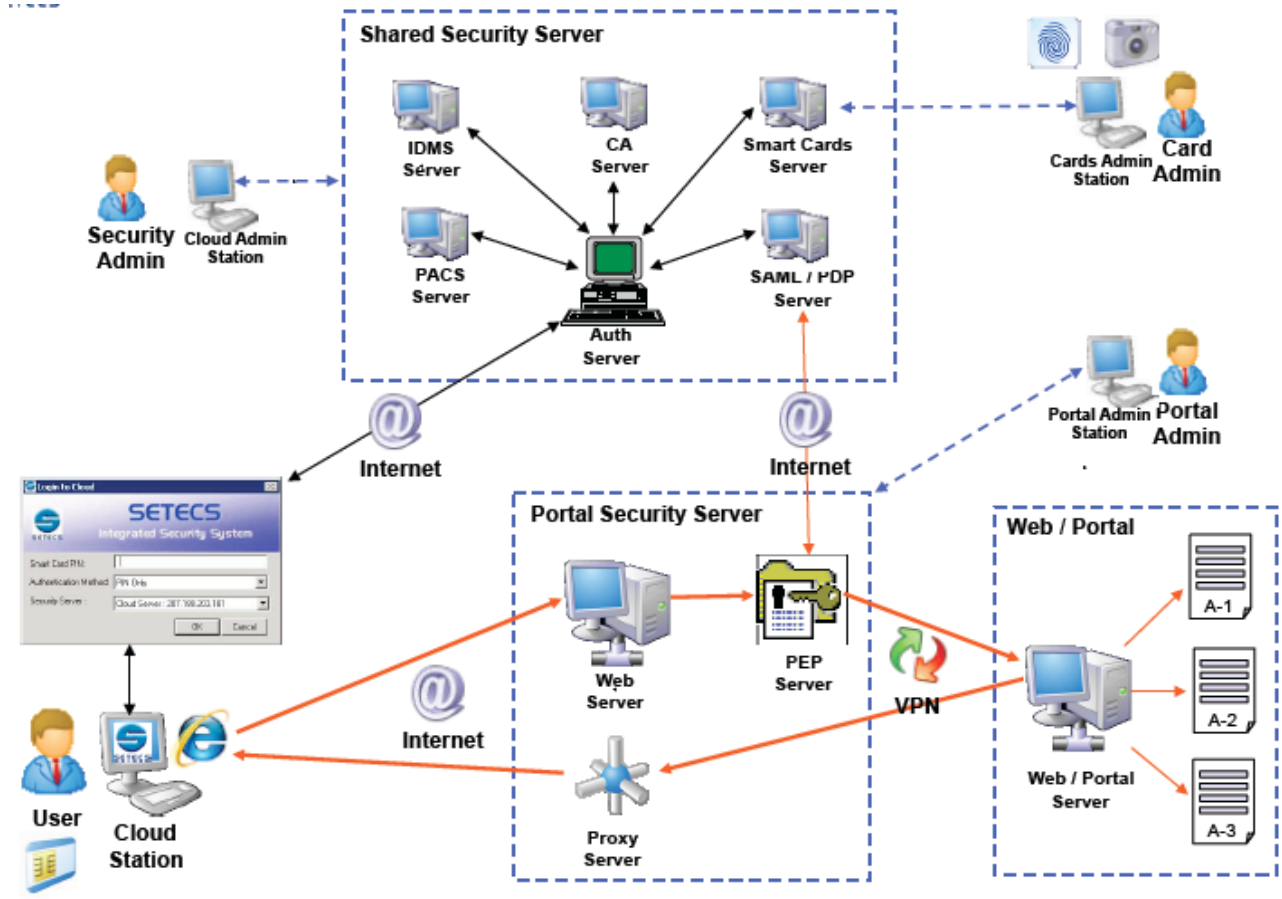

Figure 1: Shared Security Services for Web Portals

The system can also be used to protect cloud platforms. In this case the system complements and extends security features of cloud platform Hypervisors. This architecture is shown in the following Figure:

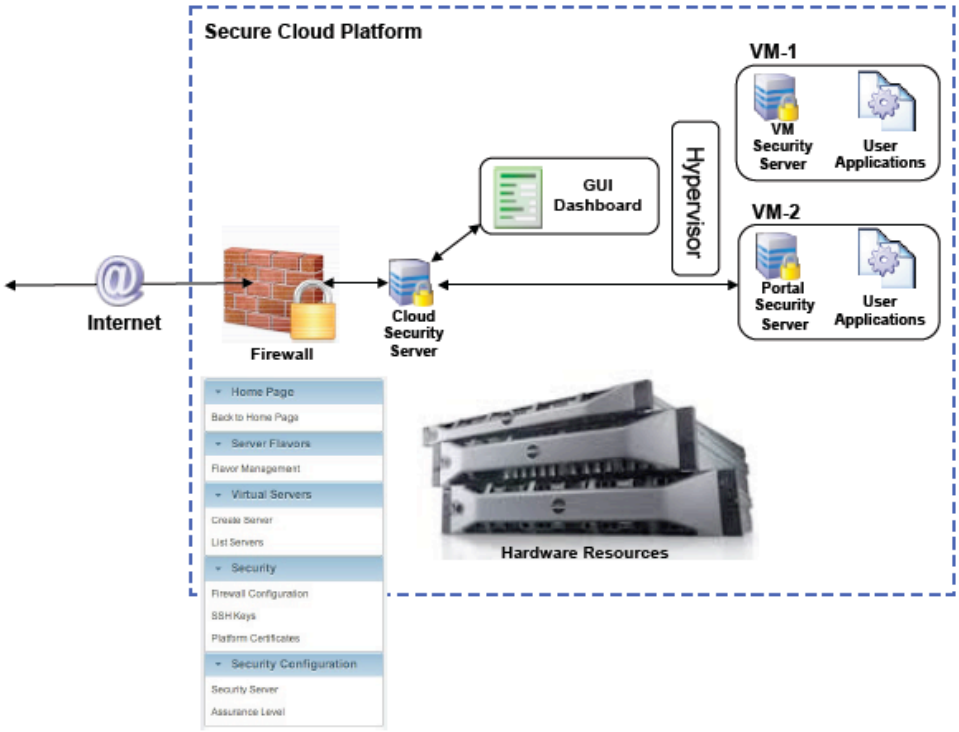

Figure 2: Security Extensions of Cloud Platforms

3. SETECS® ICAM System – Functions and Security Services

3.1 Remote User Authentication Protocol – Login to Security Access Point

In our system remote user authentication may be performed either as standard Windows remote authentication (authentication into Windows domain) or as our extended authentication (authentication into the cloud). In both cases, our generic user authentication module supports certificate-based authentication. With authentication into the Windows domain, our login module fetches PIV authentication certificate from a FIPS-201 (PIV) based smart card and presents it to the Windows login module for domain level authentication. As it is well–known, the prerequisite for such authentication is that PIV certificate must be issued by Microsoft (or compliant) CA server, the certificate must have strictly required values of the `keyUsage` attribute, and it must be stored in Microsoft's Active Directory.

Another remote authentication protocol that our system supports is authentication with the cloud's Security Access Point using mutual strong authentication protocol. Our protocol is an extension of the FIPS-196 strong authentication protocol. Its extended security functions are verification of certificates by the Local Certificate Authority (LCA) Server and verification of identities by the IDMS Server. Our mutual strong authentication protocol also uses PIV credentials and smart card-based cryptographic functions.

3.2 Single-Sign-On Protocol – Login to The Cloud

When client wants to send request to some secure Application Server in the cloud, single sign-on protocol is initiated. This protocol is slightly different in a cloud environment, compared to the standard client-server environment. Namely, in the client-server environment, client access application server directly. Therefore, each Virtual Machine Server (application server) must be extended with the associated VM Security Server (see Figure 2).

But, in cloud computing environment, the situation is different, since user does not access application servers directly. Each request is first received by the Cloud Security Server (CSS) (see Figure 2). Therefore, single sign-on protocol is performed by the CSS Server. That Server initiates single-sign-on protocol. Upon receiving the initiation message, client fetches SAML Token from a smart card and digitally signs it using private key corresponding to the digital signature certificate. It sends SAML Token to the Policy Enforcement Point – PEP (proxy associated with the Virtual Machine Security Server) along with digital signature certificate.

VM Security Server re–directs the token to the Policy Decision Point (PDP), the component of the Shared Security Server. PDP verifies both signatures. Successful verification of signatures proves that the SAML ticket was received from the PEP and presented by the owner of the SAML Ticket, which provides source authentication. After this, PDP Server consults SAML-Ticket database, in order to validate the ticket. If *OK*, it sends `SAMLAuthenticationResponse` message to the PEP Server, which contains PDP's authentication decision.

If the decision is *Deny*, VM Security Server informs the client that specific request has not been approved and terminates the connection without any further correspondence. If the decision is *Permit*, VM Security Server establishes secure session with the client.

3.3 Authorization Protocol – Role-Based Access Protocol

Authorization policies in the SETECS® Cloud Security System are based on the XACML standard. It supports Role-Based Access Control model, so an authorized person creates a group based on roles and assigns roles to users. Then Security Administrator creates rules by specifying access privileges for each group (role) along with permitted actions. Administrator then collects different rules into a Policy Token (Policy Set), which includes *Target* objects used to identify the role of each user in a group. *Target* contains the role, the name of a resource, and actions permitted to be performed by a group member with the specified resource. In addition, the Administrator can also specify *Policy* and *Rules* objects, if needed. The Administrator saves newly created policy in an XACML policy file.

When an authenticated user requests an access to a specific resource in the cloud, its client fetches SAML ticket from a smart card and sends it to the VM Security Server, along with the name of the requested resource. VM Security Server creates `SAMLAuthorizationRequest` message and sends it to the PDP Server. PDP Server consults XACML policy file and generates `SAMLAuthorizationResponse` message, which contains authorization decision. `SAMLAuthorizationResponse` is sent back to the SAP Server in order to dispatch request to an appropriate application server in the cloud, if the decision was Permit or to reject the request otherwise and return notification to the user.

3.4 Secure Sessions – Documents and Messages in Transfer

In the current version of our system secure session is established after single-sign-on protocol is successfully completed. SAP Server requests `KeyExchange` certificate from a client. The purpose of the `KeyExchange` certificate is to securely exchange session-key and session-id between a client and the VM Security Server. To manage secure sessions' attributes by the VM Security Server, the server creates an active session object for the specific client in a session's container. Each object in the session container contains the identity of the authenticated client, session key, and session ID.

Upon receiving certificate request, client fetches `KeyExchange` certificate from a smart card and sends it back to the VM Security Server. Since single-sign-on protocol is capable to authenticate clients in a distributed environment, there is still a possibility that the attacker may launch replay or impersonation attacks by presenting valid SAML ticket. To counter such attacks, VM Security Server receives `KeyExchange` certificate and compares its Distinguished Name with the identity stored in the session container. In addition, VM Security Server also verifies the certificate chain. Upon successful verification, VM Security Server generates a session-symmetric-key and session id which is digitally signed by using private key corresponding to its own digital signature certificate and enveloped using public key corresponding to the `KeyExchange` certificate of the client. It then sends session key exchange message to the client.

Client receives the message and verifies the signature. Upon successful verification, it opens the envelope using private key corresponding to the `KeyExchange` certificate in order to extract session-symmetric-key and session id. Client stores both session attributes in the Security applet of the smart card. Otherwise, it stores them in a key-file. Client uses session-symmetric-key and smart card-based cryptographic functions to create secure messages in the standard format – *PKCS*#7SignedAndEnvelopedData. The purpose of session-id is to enable later application servers to perform secure asynchronous communication with the client.

3.5 Secure Cloud Application Services – Protection of Application Resources

In our implementation of the secure cloud-computing environment, all servers located in the cloud are strongly protected and communications between them are also strongly protected. Security of internal cloud servers and their mutual protocols is described in additional white paper. Under those conditions, establishment of end–to–end secure sessions between users and application servers is in fact two-step security: the first step is external secure session established between clients at user workstations and SAP Server and the second step is secure sessions internal in the cloud established between CAP Server and application servers.

This arrangement for two-step end–to–end security is one of essential differences between cloud security and client-server security. In a client-server environment, clients access application servers directly, perform authentication or single sign-on with those servers and in that process shared session keys can be established. In a cloud-computing environment, clients do not access application servers directly. Their requests are received by the VM Security Server that analyses them and based on different parameters and conditions directs those requests to appropriate application servers located in the cloud. Thus, in principle, at the time when accessing the cloud, users and the VM Security Server do not know which application servers will be accessed later, during user's session.

This means that during initial client authentication to the cloud, secure session can be established only between the client and Cloud Security Server. Later, for secure access to application servers two approaches are possible:

- Combined secure session, comprising of one portion between the client and the Cloud Security Server and the other portion between that Server and the VM Security Server associated with the Application Server selected to serve particular request; or
- Single secure session between the client and selected application server, in case of multiple repetitive requests.

The first option introduces performance overheads due to decryption/encryption that has to be performed for each request and response by the Cloud Security Server. The second option is more efficient, but requires an intermediary step – "tunneling" protocol between selected application server and the client. The essence of that protocol is the following: during remote authentication to the cloud, client sends its certificate to the Cloud Security Server. After receiving client's first request and selecting appropriate application server to service that request, Cloud Security Server appends also client's certificate to the client's request and sends it to the VM Security Server. That Server generates shared secret key and using client's certificate, envelops secret key, and appends it to its response. Thus, the client receives shared session key from the VM Security Server associated with the accessed application server and can use it for protection of messages and documents being transferred between application server an the client.