

**Identity and Access Management
Access Services 2.0 Increment 5 eSig
System Design Document**



Department of Veterans Affairs

March 2015

Version 1.1

Note: The revision history cycle begins once changes or enhancements are requested after the System Design Document has been baselined.

Date	Version	Description	Author
04/17/2015	1.1	Updated per anomalies	[REDACTED]
03/25/2015	1.0	Updated to new ProPath template and separated for eSig applicable content	[REDACTED]

Artifact Rationale

The System Design Document (SDD) is a dual-use document that provides the conceptual design as well as the as-built design. This document will be updated as the product is built, to reflect the as-built product. Per the Project Management Accountability System (PMAS) Guide, the SDD as a conceptual design is required prior to the Milestone 1 Review. (Sections 1, 2, 3, 4, 5, 7, 9 need to be populated, as applicable.) The as-built design for each delivery must be incorporated prior to the Milestone 2 Review. (The entire document needs to be populated or updated, as applicable.)

Table of Contents

1. Introduction	1
1.1. Purpose of the SDD	1
1.2. Identification	2
1.3. Scope	3
1.3.1. Increment 5 eSig Scope	3
1.4. Constraining Policies, Directives and Procedures	3
1.5. User Characteristics	6
1.6. Relationship to Other Documents and Plans	6
1.7. Definitions, Acronyms, and Abbreviations	7
1.8. References	7
2. Background	8
2.1. Overview of the System	8
2.2. Overview of the Business Process	8
2.3. Business Benefits	10
2.4. Assumptions and Constraints	10
2.4.1. Design Assumptions	10
2.4.2. Design Constraints	11
2.4.3. Design Trade-offs	11
2.5. Overview of the Significant Requirements	11
2.5.1. Overview of Significant Functional Requirements	11
2.5.2. Overview of Functional Workload/Performance Requirements	14
2.5.3. Overview of Operational Requirements	15
2.5.4. Overview of the Technical Requirements	16
2.5.5. Overview of the Security or Privacy Requirements	16
2.5.6. Overview of System Criticality and High Availability Requirements	16
2.5.7. Single Sign-on Requirement	17
2.5.8. Requirement for Use of Enterprise Portals	17
2.5.9. Special Device Requirements	17
2.6. Legacy System Retirement	17
3. Conceptual Design	18
3.1. Conceptual Application Design	18
3.1.1. Application Context	18
3.1.1.1. eSignature	20
3.1.2. High-Level Application Design	21
3.1.3. Application Locations	23
3.2. Conceptual Data Design	23
3.2.1. Project Conceptual Data Model	23

3.2.2.	Database Information	24
3.2.3.	User Interface Data Mapping	24
3.2.3.1.	Application Screen Interface	25
3.2.3.1.1.	CoSign CA Certificate	25
3.2.3.2.	Application Report Interface.....	26
3.2.3.3.	Unmapped Data Element.....	26
3.3.	Conceptual Infrastructure Design	26
3.3.1.	System Criticality and High Availability.....	26
3.3.2.	Special Technology	27
3.3.3.	Technology Locations.....	27
3.3.4.	Conceptual Infrastructure Diagram.....	27
3.3.4.1.	Location of Environments and External Interfaces	28
3.3.4.2.	Conceptual Production String Diagram	30
4.	System Architecture	31
4.1.	Hardware Architecture	31
4.2.	Software Architecture.....	35
4.3.	Network Architecture.....	39
4.4.	Service Oriented Architecture/ESS	40
4.5.	Enterprise Architecture	40
5.	Data Design	41
DBMS Files		41
5.1.	41	
5.2.	Non-DBMS Files	41
5.3.	Data View	41
6.	Detailed Design	42
6.1.	Hardware Detailed Design.....	42
6.2.	Software Detailed Design.....	42
6.2.1.	Conceptual Design	42
6.2.1.1.	Product Perspective.....	42
6.2.1.1.1.	User Interfaces	42
6.2.1.1.2.	Hardware Interfaces	42
6.2.1.1.3.	Software Interfaces	42
6.2.1.1.4.	Communications Interfaces.....	42
6.2.1.1.5.	Memory Constraints.....	43
6.2.1.1.6.	Special Operations	43
6.2.1.2.	Product Features	43
6.2.1.3.	User Characteristics.....	44
6.2.1.4.	Dependencies and Constraints	44
6.2.1.5.	eSig Design	44
6.2.1.5.1.	Sign a Document.....	46
6.2.1.5.2.	Verify a Signed Document.....	47
6.2.2.	Specific Requirements	48
6.2.2.1.	Database Repository	48

6.2.2.2.	System Features.....	48
6.2.2.3.	Design Element Tables.....	48
6.2.2.3.1.	Routines (Entry Points).....	48
6.2.2.3.2.	Templates.....	48
6.2.2.3.3.	Bulletins.....	49
6.2.2.3.4.	Data Entries Affected by the Design.....	49
6.2.2.3.5.	Unique Record(s).....	49
6.2.2.3.6.	File or Global Size Changes.....	49
6.2.2.3.7.	Mail Groups.....	49
6.2.2.3.8.	Security Keys.....	49
6.2.2.3.9.	Options.....	49
6.2.2.3.10.	Protocols.....	49
6.2.2.3.11.	Remote Procedure Call (RPC).....	49
6.2.2.3.12.	Constants Defined in Interface.....	49
6.2.2.3.13.	Variables Defined in Interface.....	49
6.2.2.3.14.	Types Defined in Interface.....	49
6.2.2.3.15.	GUI.....	49
6.2.2.3.16.	GUI Classes.....	49
6.2.2.3.17.	Current Form.....	49
6.2.2.3.18.	Modified Form.....	49
6.2.2.3.19.	Components on Form.....	49
6.2.2.3.20.	Events.....	50
6.2.2.3.21.	Methods.....	50
6.2.2.3.22.	Special References.....	50
6.2.2.3.23.	Class Events.....	50
6.2.2.3.24.	Class Methods.....	50
6.2.2.3.25.	Class Properties.....	50
6.2.2.3.26.	Uses Clause.....	50
6.2.2.3.27.	Forms.....	50
6.2.2.3.28.	Functions.....	50
6.2.2.3.29.	Dialog.....	50
6.2.2.3.30.	Help Frame.....	50
6.2.2.3.31.	HL7 Application Parameter.....	50
6.2.2.3.32.	HL7 Logical Link.....	50
6.2.2.3.33.	COTS Interface.....	50
6.2.3.	System Maintenance Design	50
6.2.3.1.	Maintenance Pages.....	51
6.3.	Network Detailed Design.....	51
6.4.	Service Oriented Architecture/ESS Detailed Design	51
6.4.1.	Service Description for eSig.....	51
6.4.2.	Service Design for eSig.....	51
6.4.2.1.	Introduction.....	51
6.4.2.1.1.	Purpose and Scope of Service.....	51
6.4.2.1.1.	Links to Other Documents.....	51
6.4.2.2.	Service Details.....	51
6.4.2.2.1.	Service Identification.....	51
6.4.2.2.2.	Service Versions.....	51
6.4.2.2.3.	Summary of Design and Platform Details.....	51
6.4.2.2.3.1.	SOA Pattern(s) Implemented.....	51

6.4.2.2.3.2.	COTS Platform vendor names and versions for hosting platform.....	51
6.4.2.3.	Dependencies.....	52
6.4.2.4.	Service Design Details.....	52
6.4.2.4.1.	Interface Technical Specs	52
6.4.2.4.1.1.	Service Invocation Type	52
6.4.2.4.1.2.	Service Interface Type	52
6.4.2.4.1.3.	Service Name	52
6.4.2.4.1.4.	Interface	52
6.4.2.4.1.5.	End Points	52
6.4.2.4.1.6.	Operations or Methods.....	52
6.4.2.4.1.7.	Message Schemas	52
6.4.2.4.2.	Information Model	52
6.4.2.4.2.1.	Class Diagram and Description of Entities Involved.....	52
6.4.2.4.2.2.	Mappings from ELDM to Standards Based Schemas.....	52
6.4.2.4.3.	Behavior Model (AKA Use Case Realization)	52
6.4.2.4.3.1.	Use Cases (Use Case Model)	52
6.4.2.4.3.2.	Interaction Diagrams	52
6.4.2.5.	Gap Analysis	52
6.4.2.5.1.	Variances from Enterprise Target Architecture	53
6.4.2.5.2.	Variances from SLDs.....	53
6.4.2.5.3.	Variances from Standards and Policies.....	53
6.4.2.5.4.	Justification for Exceptions and Mitigation	53
Sign		53
6.4.3.	53	
6.4.4.	Verify	53
6.4.5.	Delete	54
7.	External System Interface Design	55
7.1.	Interface Architecture.....	55
7.2.	Interface Detailed Design	55
8.	Human-Machine Interface	56
8.1.	Interface Design Rules	56
8.2.	Inputs	56
8.3.	Outputs	56
8.4.	Navigation Hierarchy.....	56
8.4.1.	Screen Shots.....	56
9.	Security and Privacy	57
9.1.	Security.....	58
9.2.	Privacy	58
9.2.1.	Confidentiality of Sensitive Information	58
9.2.2.	Privacy of Personal Information	58
9.2.3.	Process Integrity.....	58
9.2.4.	System Availability	58
	Attachment A – Approval Signatures	60

A. Additional Information.....	61
A.1. RTM.....	61
A.2. Packaging and Installation.....	61
A.3. Design Metrics	61
A.4. Acronym List and Glossary	61
A.5. Required Technical Documents	61
A.6. Attach Documents	61

DRAFT

1. Introduction

The Department of Veterans Affairs (VA) currently serves Veterans, their beneficiaries, and other VA stakeholders via services across many distributed and often operationally disjoint Lines of Business (LOB). Though VA serves the stakeholders across a vast enterprise of internal and external businesses and programs, it currently lacks a single, uniform method for identifying stakeholders and applying Access Management Services to safeguard its information resources. VA also lacks the capability to harmoniously share and leverage sensitive information across its internal LOBs and external business partners. Based on this existing operating model, the Veterans Relationship Management (VRM) Program Management Office (PMO) has identified the need to establish core Access Services (AcS) to definitively and consistently identify VA stakeholders and to establish supporting processes that increase the level of security protecting the identities, information, and interests of VA stakeholders.

The enterprise-wide system as a whole is referred to as the VA AcS 2.0, which includes the applicable subcomponents. The individual subcomponents or groups are referred to as a VA AcS activity or the VA AcS activities. The VA AcS activities include the following:

Single Sign-On – Internal (SSOi)	Identity Proofing (IP)
Single Sign-On – External (SSOe)	Provisioning (PROV)
Credential Service Provider (CSP)	Specialized Access Control (SAC)
Electronic Signature (eSig)	Compliance Audit and Reporting (CAR)

Within each of the AcS activities, commercial off-the-shelf (COTS) products are used to enable the specific capabilities of the AcS 2.0 described in this document and identified by the business as referenced (where applicable) in the Business Requirements Document (BRD) and Requirements Specifications Document (RSD). The AcS 2.0's primary customers are both internal and external user communities who need logical access to VA business applications. VA is required to provide eSignature (eSig) capabilities to be used by our nation's Veterans, VA business partners, and other persons of interest who conduct business electronically with VA. This capability greatly improves the Veteran's and business partners' experience by reducing the need for the use of traditional mail and the need to be physically present at a VA facility to sign documents. By implementing this technology, VA has improved the end user experience, and realized internal efficiencies by reduction of paper processes. The solution is scalable to support a minimum of 10 million external users. Electronic signature (eSig) is a method of signing an electronic message that identifies and authenticates a particular person as the source of the electronic message. It indicates such person's approval of the information contained in the electronic message.

1.1.Purpose of the SDD

The purpose of the System Design Document (SDD) is to describe the supporting mechanics of the eSig solution. The SDD translates the requirement specifications into a document from which the developers may create the technical solution. It identifies the top-level system architecture, as well as the supporting hardware, software, communication, and interface components. This artifact is an evolving document and is a living artifact that is updated (as applicable) when modifications are incorporated and/or new capabilities are added to the solution (when appropriate).

The primary target audience is eSig developers and teams who will assist in the establishment of the infrastructure, as well as the following stakeholders:

- VA, Department of Defense (DoD), business partners, and other federal agencies
- AcS 2.0 Architects
- AcS 2.0 Business Sponsors
- Developers and technical managers
- Senior management and mission owners who enforce decisions about the IT security budget
- IT security program managers, who implement the security program
- Information System Security Officers (ISSO) responsible for IT security
- IT application owners of software and/or hardware used to support AcS activities
- Information owners of data stored, processed, and transmitted by the IT applications
- Other technical support personnel and product vendors

This document provides the solution architecture and detailed design of the eSig solution as well as details for understanding the specific system configurations, interfaces, workflow, Graphical User Interfaces (GUI), and data models. The purpose of this document is to describe in sufficient detail how the proposed eSig system is to be constructed. The System Design Document (SDD) translates the Requirement Specifications into a document from which the developers can create the actual system. It identifies the top-level system architecture, and identifies hardware, software, communication, and interface components.

1.2. Identification

The information contained herein is based on the ARX and Oracle COTS products to provide the core capabilities for access control services to VA stakeholders. This document applies to the following systems and software:

Table 1: System Identification

Name	Description	Abbreviation	Version	Release
CoSign ARX	Electronic signature (eSig) is a method of signing an electronic message that identifies and authenticates a particular person as the source of the electronic message.	eSig	V5.X	NA

1.3.Scope

This SDD focuses on the technical system design to provide the foundation for the eSig solution. It provides an overview of the core capabilities, architecture, and design. It does not include default COTS product design nor does it include OOTB data definitions, tables, or models except where the design alters such elements and components. The sections below provide scope inclusion and exclusion details.

Table 2: Scope Inclusions

Includes
<ul style="list-style-type: none"> Provides capability to electronically sign and verify documents using web service based task Provides support for documents types –Word and PDF Provides eSig enrollment services to allow the eligible external users for VA internal applications to sign the document. eSig is limited to external persons of interest, Veterans or non-Veterans that do not have credentials that carry signing certificates (hard token or soft token) Provides functionality to delete user access

Table 3: Scope Exclusion

Excludes
<ul style="list-style-type: none"> Does not require a GUI, thus it does not provide registration screens for a user User authentication is the responsibility of individual VA application Does not support PowerPoint and client based email signing capability due to limitation of product Does not integrate with a third party Certificate Authority (CA)

1.3.1. Increment 5 eSig Scope

There are no eSig Enterprise requirements for this AcS 2.0 Increment 5.0increment.

1.4.Constraining Policies, Directives and Procedures

This design complies with the following policies, directives, and procedures (as applicable). The specific requirement and sub-requirement numbers are highlighted in the individual service-specific SDDs (where appropriate). Applicable directives for the eSig solution include but are not limited to the National Institutes of Standards and Technologies (NIST) issued guidelines

800-53, 800-63, and Federal Information Processing Standard (FIPS) 140-2. Under the Federal Information Security Management Act (FISMA), federal government agencies are required to adhere to the security controls as described in the NIST guidelines. Other policies, directives and procedures that are applicable to the AcS services are listed below.

Table 4: Policies, Directives, and Procedures

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
1	VA	VA 6500 Handbook	<ul style="list-style-type: none"> • Directive Information Security Program. • Defining overall Security Framework for VA.
2	VA	VA 6501 Directive	<ul style="list-style-type: none"> • VA Identity Verification In-Person Proofing (IPP) Process. • Defining overall Identity Proofing Methodology for VA IAM.
3	VA	VA 6300 Directive	<ul style="list-style-type: none"> • Directive Records and Information Management. • Defines information management framework for VA Access Services.
4	NIST	SP 800-53-4	<ul style="list-style-type: none"> • Special Publication – Recommended Security Controls for Federal Information Systems and Organizations. • Defines the required security controls for IT systems under the Federal Information Security Management Act (FISMA).
5	NIST	SP 800-63-2	<ul style="list-style-type: none"> • Special Publication – Electronic Authentication Guideline. • Defines levels of assurance in user identities presented to IT systems over open networks. • Defines the data and procedural requirements for VA Access Services.
6	NIST	FIPS-201-2	<ul style="list-style-type: none"> • Federal Information Processing Standards Publication – PIV of Federal Employees and Contractors. • Provides Identity Proofing, credentialing and chain of trust requirements and processes. • Defines the method for secure administrative interaction and control.
7	NIST	FIPS-140-2	<ul style="list-style-type: none"> • Federal Information Processing Standards Publication (FIPS) – Security Requirements for Cryptographic Modules. • Defines the cryptographic standards and requirements.

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
8	NIST	SP 800-122	<ul style="list-style-type: none"> • Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). • Provides technical procedures for protecting PII in information systems. • Defines the information which can be used to distinguish or trace an individual's identity.
9	US Congress	Section 508 Amendment to the Rehabilitation Act of 1973	<ul style="list-style-type: none"> • Section 508 Electronic and information technology requirements for Federal departments and agencies. • Accessibility, development, procurement maintenance, or use of electronic and information technology. • Defines the "Human-Machine Interface" accessibility requirements.
10	OMB	M-04-04	<ul style="list-style-type: none"> • Memorandum to the Heads of All Department and Agencies – E-Authentication Guidance for Federal Agencies. • Defines the E-Authentication requirement.
11	OMB	M-11-11	<ul style="list-style-type: none"> • Requirements for Accepting Externally-Issued Identity Credentials. • FICAM architecture and procedures for federal agencies.
12	GSA	FICAM	<ul style="list-style-type: none"> • Federal Identity, Credentialing and Access Management (FICAM) Roadmap and Implementation Guidance. • Provides the common segment architecture and implementation guidance for federal ICAM programs.
13	White House	NSTIC	<ul style="list-style-type: none"> • National Strategy for Trusted Identities in Cyberspace (NSTIC) – Provides guidance for identity trust in cyberspace.
14	US Congress	FISMA	<ul style="list-style-type: none"> • FISMA of 2002, Public Law 107-347
15	US Congress	E-Government Act of 2002	<ul style="list-style-type: none"> • Federal Management and Promotion of Electronic Government Services. • Defines the requirements for electronic services.
16	US Congress	The Privacy Act of 1974	<ul style="list-style-type: none"> • § 552a. Records maintained on individuals. • Defines VA Access Services Privacy assessment and control requirements.

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
17	National Archives and Records Administration (NARA)	Federal Records Act	<ul style="list-style-type: none"> Establishes the framework for records management programs in Federal Agencies.
18	VA	VA D 0735	<ul style="list-style-type: none"> Homeland Security Presidential Directive 12 (HSPD-12) Program Defines Department-wide policy, roles, and responsibilities for the creation and maintenance of systems and processes to implement VA's HSPD-12 Program necessary to implement Homeland Security Presidential Directive 12 (HSPD-12) program.
19	OMB	M-05-24	<ul style="list-style-type: none"> Implementation of HSPD 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.

1.5. User Characteristics

The users of the eSig service include a diverse constituency of VA to include Veterans and dependents with approved credentials. Only Veterans who have completed the appropriate level of identity proofing will have access to the digital signature capability.

Additional users include operational and administrative users. These are persons identified and authorized as the eSig interfacing VA Application Administrator with rights to perform administrative functions for the eSig Service, including systems configuration, modifying user accounts, as well as performing and defining reporting and auditing functions.

Enrollment to the eSig Service is automatic for a user with the appropriate credential levels. The first time a Veteran with an L2 or higher credential attempts to sign a document, the eSig Service determines if the user ID exists. If the user is not found, they are automatically enrolled into eSig utilizing PKI and allowed to sign the document.

1.6. Relationship to Other Documents and Plans

The system design outlined in this document should be used along with the functional requirements specified in the Increment 5 AcS Requirements Specification Document (RSD).

The system design is developed based on the progressive refinement and discovery of business and functional requirements outlined and extracted from the following documents, which are located on the [AcS TSPR](#) site.

Note: The applicable standards and guidelines from the VA Handbook and NIST are identified in section 1.5 above.

1.7.Definitions, Acronyms, and Abbreviations

The abbreviations and terms used in this SDD are defined in the [Identity and Access Services Master Glossary](#).

1.8.References

The document references are listed in Section 1.6 above.

DRAFT

2. Background

VA wishes to implement eSig capabilities to be used by our nation's Veterans and other persons of interest who perform business electronically with the VA. This capability will greatly improve the Veteran's experience by negating the need for the use of traditional mail and the need to be physically present at a VA facility to sign documents. By implementing this new technology, VA anticipates not only improving the Veteran experience, but also realizing improved internal efficiency by reduction of paper processes. Design and implementation of supporting components (i.e., a Forms Service), if they do not already exist within the VA and/or are not scalable to support this eSig solution may be necessary. The solution must be scalable to support approximately 10 million Veterans.

2.1. Overview of the System

The purpose of the VA AcS Development Support task is to design, develop, implement, integrate, operationalize, and sustain an enterprise-wide VA AcS 2.0 for VA VRM. In order to coordinate AcS across several VRM work streams, multiple internal and external systems will need to be interconnected to provide access to these systems by facility, system and individual entities. The goal of AcS is to facilitate access transactions using an Enterprise Services framework. The Framework should address the user account lifecycle, from identity creation through de-provisioning of the user. To accomplish these goals, the AcS should consider highly available services in an effort to minimize unintentional disruptions for the users.

This document provides the underlying design to support the eSig activities. The system design is based on a Service Oriented Architecture (SOA) approach. The solution architecture uses accepted COTS products for each of VA AcS activity and applies the leading practices as outlined by the product vendor to the extent possible. The design of the architecture supports VA's scalability, security, extensibility, and high availability requirements to provide a flexible enterprise solution.

2.2. Overview of the Business Process

The AcS 2.0 is made up of several activities, which are necessary to provide identity and access management services to both internal VA employees/contractors and to external end users. It provides VA applications centralized authentication mechanism for internal users and federation capabilities to access external application. Authorization capabilities to provide coarse- and fine-grained application access while providing workflow for self-service account requests, approvals, and user life cycle management.

VA is required to provide eSig capabilities to be used by our nation's Veterans, VA business partners, and other persons of interest who conduct business electronically with VA. This capability greatly improves the Veteran's and business partners' experience by reducing the need for the use of traditional mail and the need to be physically present at a VA facility to sign documents. By implementing this technology, VA has improved the end user experience, and realized internal efficiencies by reduction of paper processes. The solution is scalable to support a minimum of 10 million external users.

The eSig service provides VA applications capability to digitally sign PDF and Word documents. The application is for external VA users and once the application has authenticated the user, it will allow the user to digitally sign the document thus eliminating the need to print, sign and

mailing the document. In addition, the service also allows the applications to perform admin functions to manage the lifecycle of the eSig identity

Refer to the [Use Case Model](#) for AcS and [eSig](#) for additional applicable diagrams to support this section. Below is the eSig Process Flow diagram:

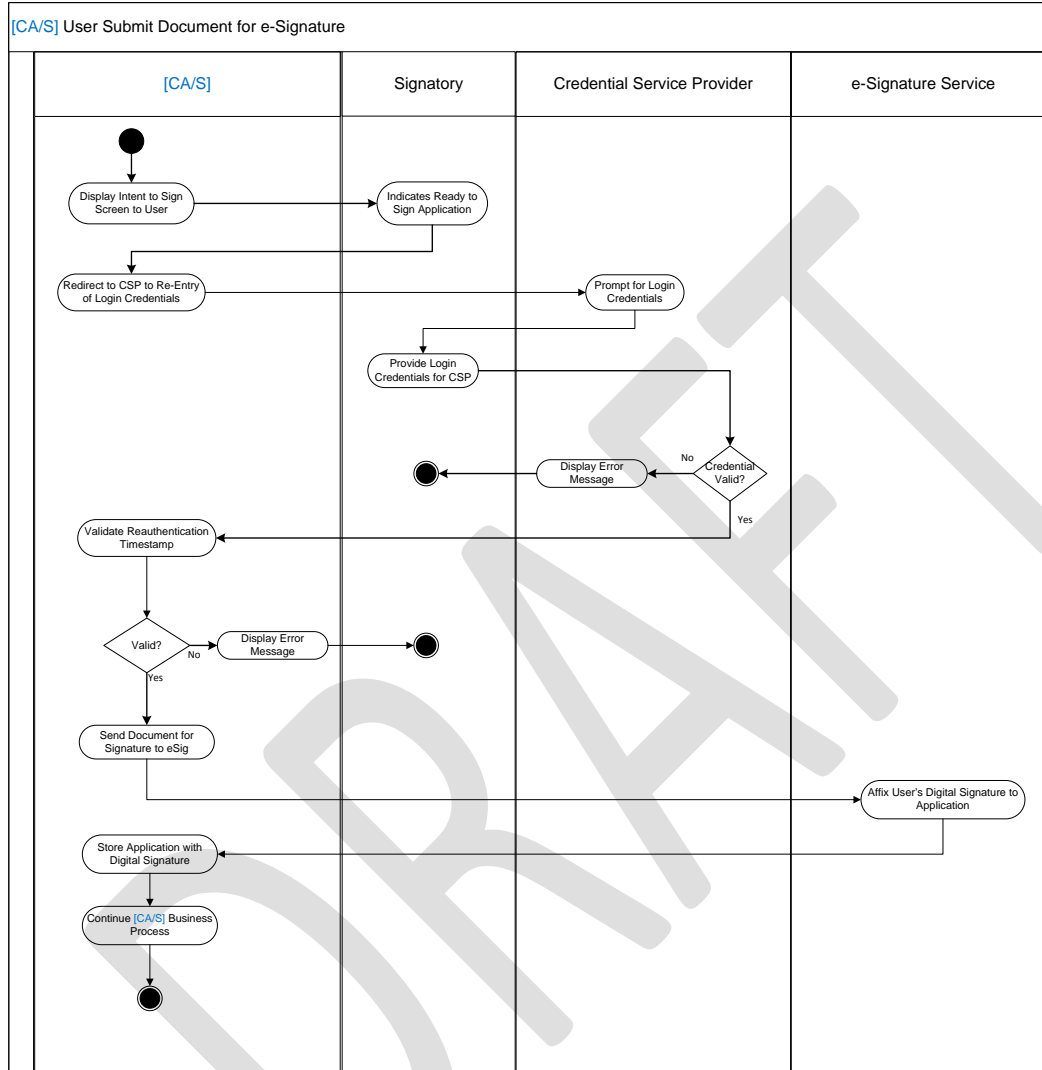


Figure 1: eSig Process Diagram

eSignature (eSig): VA is required to offer eSignature capabilities to perform business electronically. This capability reduces the need for the use of traditional mail and the need to be physically present at a VA facility to sign documents. With this new technology, VA anticipates not only improving the Veteran experience, but also realizing improved internal efficiencies by reduction of paper processes. These goals are achieved through the implementation of the eSig service.

Table 5: Functions/Patterns Supported

Function (Use Case)	Description
AcS i4 Use Case Model	I4 Use Case Model
AcS 2.0 Solution UC Model eSig	eSig Use Case Model

The applicable eSignature Use Cases are listed below:

- Sign a Document
- Check User Registration
- Validate Document
- Remove User Access

Table 6: Business Processes

Business Process ID	Business Process Name	Type	Owner	Description
1	Register for a Signing Certificate	Modernized	IAM	When a user needs to electronically sign a document, but does not have a digital certificate, the user must register to obtain the certificate.
2	Sign a Document with an Existing Certificate	Modernized	IAM	A user can electronically sign a document with an existing digital certificate.
3	Verifying a Signature	Modernized	IAM	A user can verify an electronic signature on a previously signed document.

2.3. Business Benefits

Veterans and their dependents will be provided with a user-friendly tool to perform self-service form signatures on-demand reducing the burden brought on with paper based signature forms.

2.4. Assumptions and Constraints

2.4.1. Design Assumptions

Users of the eSig service will be authenticated via SSOe at LOA2 or greater, commensurate with the form data presented by the application. This section describes the assumptions and constraints that impact the design of the eSig solution.

Table 7: Assumptions and Constraints

Assumption/Constraints
<ul style="list-style-type: none">• The eSig functionality will be consumed only by external users. Internal users will use their PIV card to sign the documents.• The VA Consuming Application(s) will be responsible for authenticating the users. Mutual trust will be established between VA applications and eSig activity.• The end point applications are responsible for the authentication process (LOA2 or higher) and user identity lifecycle• There is no access control list for the ARX CoSign device.• The eSig activity does not provide document hosting service(s).

Assumption/Constraints

- The eSig solution does not provide a federated environment.
- Since eSig depends on federated credentials, it is not possible to know if a credential has been revoked by the identity provider, thus triggering a removal of the user's signature capability. As a result, eSig will expose a 'remove user' service for dependent applications to invoke as credentials are inactivated or invalidated.
- The eSig solution does not have access to VA global LDAP/AD directory and hence needs to maintain its own user repository.
- The eSig solution does not provide administrative access to the eSig solution using PIV authentication.
- The eSig solution provides indirect ability to sign web forms through conversion of the general "web form" to a supported for signing format (Adobe Acrobat PDF, Microsoft Word, etc.).
- Horizontal scaling to increase capacity (number of users) is not a supported option for the eSig activity.

2.4.2. Design Constraints

Refer to table 7 for constraints

2.4.3. Design Trade-offs

Interoperability – The eSig acceptable formats will be PDF and MS WORD. The PDF format is an International Organization for Standardization (ISO) 32000-1 standard. With PDF files, all of the certificate data is contained within the PDF file including the x.509 certificate, data that was signed, and any other custom data captured at the time of the signing event such as a timestamp.

Usability– The eSig service is not available to the general VA public. Use of the eSig service is only available to VAAFI authenticated users through a VA application.

2.5. Overview of the Significant Requirements

This section provides an overview of the requirements that are within the scope for eSig.

2.5.1. Overview of Significant Functional Requirements

Below are the Functional Requirements that support eSig:

Table 8: Functional Requirements

eSignature – Provide a capability for users to digitally sign electronic forms during the signing process instead of scanning them from paper.			Medium	FY14 8/15/2013
13.01	eSignature Service shall accept a request to apply an eSignature.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.02	eSignature Service shall receive the unique User token.	FICAM v2, Section 8.5.2	Medium	FY14 8/15/2013
13.03	eSignature Service shall retrieve the user private key.	FICAM v2, Section 8.5.2	Medium	FY14 8/15/2013

eSignature – Provide a capability for users to digitally sign electronic forms during the signing process instead of scanning them from paper.			Medium	FY14 8/15/2013
13.04	eSignature Service shall apply the eSignature.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.05	eSignature Service shall have the capability to apply a date stamp when the eSignature is applied.	FICAM v2, Section 8.5.2	Medium	FY14 8/15/2013
13.06	eSignature Service shall have the capability to apply a time stamp when the eSignature is applied.	FICAM v2, Section 8.5.2	Medium	FY14 8/15/2013
13.07	eSignature Service shall notify User of unsuccessful eSignature attempt.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.08	eSignature Service shall notify the Application of unsuccessful eSignature attempt.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.09	eSignature Service shall have the capability to optionally apply application specific properties.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.1	eSignature Service shall automatically enroll the User at the intent to sign.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.11	eSignature Service shall receive a User token for enrollment.	FICAM v2, Section 8.5.2	Medium	FY14 8/15/2013
13.12	eSignature Service shall create a User key pair and public key certificate.	FICAM v2, Section 8.5.2	Medium	FY14 8/15/2013
13.13	eSignature Service shall receive a disenrollment request.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.14	eSignature Service shall revoke User public certificate.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.15	eSignature Service shall archive User key pair and public key certificate.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.16	eSignature Service shall receive request for Standard report from the request log.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.17	eSignature Service shall provide the ability to identify data elements on which	FICAM v2, Section 9.4	Medium	FY14 8/15/2013

eSignature – Provide a capability for users to digitally sign electronic forms during the signing process instead of scanning them from paper.			Medium	FY14 8/15/2013
	to report.			
13.18	eSignature Service shall provide a notification that request was received.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.19	eSignature Service shall provide a notification when a report error has occurred.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.2	eSignature Service shall provide specific error message.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.21	eSignature Service shall provide the properly authorized user the ability to schedule the required report.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
13.22	eSignature Service shall provide the ability to customize report parameters.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
13.23	eSignature Service shall provide the ability to store customize report parameters.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.24	eSignature Service shall process requested Standard report.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
13.25	eSignature Service shall compile requested data elements.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.26	eSignature Service shall produce report within scheduled parameters.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
13.27	eSignature Service shall provide the ability to automatically generate scheduled standard reports.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
13.28	eSignature Service shall save the report in exportable file format.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.29	eSignature Service shall save the report in a PDF file format.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.3	eSignature Service shall save the report in a CSV file format.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013

eSignature – Provide a capability for users to digitally sign electronic forms during the signing process instead of scanning them from paper.			Medium	FY14 8/15/2013
13.31	eSignature Service shall save the report in a text file format.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.32	eSignature Service shall deliver requested Standard report to Requestor.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.33	eSignature Service shall deliver a report on identified data elements to Requestor.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.34	eSignature Service shall deliver report in a PDF file format.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.35	eSignature Service shall deliver a report in a CSV file format.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.36	eSignature Service shall deliver a report in a text file format.	IPT Approved (2012) eSig Business Packets	Medium	FY14 8/15/2013
13.37	eSignature Service shall deliver a report within scheduled parameters.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
13.38	eSignature Service shall deliver a report within identified date range.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
13.39	eSignature Service shall deliver a report based on action taken.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
13.4	eSignature Service shall deliver a report based on volume of activity.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
13.41	eSignature Service shall deliver a report based on source of request.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
13.42	eSignature Service shall deliver a report based on rejected request.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
13.43	eSignature Service shall support the ability to have multiple signatures.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013

2.5.2. Overview of Functional Workload/Performance Requirements

As per Section 2.9 from the AcS 2.0 RSD, the performance specifications are targeted for the planned consumption of AcS services for the following year; however, the performance specifications are easily scalable for future implementations. The performance specifications include the following:

- a. The online application screens contained in the user interface render less than ten seconds with an average rendering of three seconds within the budgeted resource utilization constraints.

- b. The online procedures prompted from a user interface execute under five seconds with an average of four seconds within the budgeted resource utilization constraints.
- c. The metric data indicating the performance characteristics of the system to support application monitoring is provided.

2.5.3. Overview of Operational Requirements

Per Section 2.11 of the AcS 2.0 RSD, AcS solution is operational and hosted within the Terremark environment as required by VA. Terremark, the Data Center Team and the AcS Sustainment Team are responsible for the reliability and monitoring of solution. The tools, methods, and specifications for monitoring the reliability of the AcS solution are at the discretion of Terremark, the Data Center Team and the AcS Sustainment Team.

Table 9: Service Availability Level 4

***Standards adopted from specification created by Application Structure and Integration Services (ASIS)	
Description	Mission Critical Information
Minimum Availability	99.99%
Maximum Downtime Per Month	4.4 minutes
Business Value	Essential to fundamental business operations – outage seriously impairs functioning of business.
System Response	In the absence of any system superseding requirements, the system responds to user actions in three seconds or less in 90% of the attempts, and never more than 10 seconds.
Operational Hours	Required 24 hours a day, every day.
Significant Outage	More than five minutes of downtime is considered significant at any time and requires an ANR to be sent out to the appropriate teams.
Outage Impact	Interruption of service may result in severe financial, regulatory, patient safety, patient health, or other business issues.
Scheduled Maintenance	Maintenance, including maintenance of externally developed software incorporated into the IAM system, is scheduled during off-peak hours (evenings and weekends) or in conjunction with relevant maintenance schedules.

2.5.4. Overview of the Technical Requirements

Awaiting RTM from the Rational Team Concert Tool.

2.5.5. Overview of the Security or Privacy Requirements

As per Section 2.13 of the AcS 2.0 increment 5 RSD, the security specifications include the following:

- AcS is deployed inside the VA firewall.
- AcS conforms to the VA security standards detailed in VA Handbook 6500 Information Security Program.
- Designated ports are opened between systems. All other ports are blocked to provide secure server-to-server communication.
- The Hypertext Transfer Protocol Secure (HTTPS) communication protocol is used for outbound and inbound traffic for external-facing applications.
- AcS communication channels are TLS/Secure Sockets Layer (SSL)-enabled and -encrypted.
- The AcS data layer is within the internal firewall zone to provide security of the data.
- AcS meets all Veterans Health Administration (VHA) security, privacy, and identity management requirements and those listed in VA Handbook 6500 (Enterprise Requirements Appendix).
- AcS databases, user information stores, and information tied to individuals are secured and/or encrypted while at rest and in motion.
- Access to the administrative, management, and internal user interfaces of the authorization service is controlled through the use of SSOi.
- The system must store and transmit Personally Identifiable Information (PII) or sensitive information such as passwords in an encrypted or one-way hashed format and on the SSL channel.
- The web servers providing access to VA applications for external users over the Internet must reside in the demilitarized zone (DMZ).

Table 10: Security Requirements

ID	Requirement
1	ESig service requires an authority to operate (ATO) granted through the VA Certification & Accreditation (C&A) process. eSig will adhere to the VA C&A process and properly document the maintenance approach within the Program Management Accountability System (PMAS) artifacts.

2.5.6. Overview of System Criticality and High Availability Requirements

The VA AcS infrastructure supports critical business systems. The current availability requirement for mission critical systems is 99.9%. The current data centers support 99.6% availability. The Production, Preproduction, and Disaster Recovery (DR) Data Center is hosted by Terremark in Culpeper, Virginia and Miami, Florida. Terremark does not currently support an

active/active geographic failover and load balancing thus failover to the DR site could take between one (1) and eight (8) hours. To mitigate the risk of not having a complete site failover, the AcS production infrastructure is intended to be scalable with limited single points of failure. The primary production platform is virtualized with a physical servers dedicated to Oracle RAC and VDS.

The DR site is contingency site that will resume data center operations in the event of a site failure. Load balancing, fault tolerance, backups and archiving, is a function of the hosting facility, Terremark and the data center operations team. Backups are described more fully in the [Production Operations Manual \(POM\)](#), but essentially are the following:

- Full backups are taken of virtual machines on a weekly basis
- Backups of virtual machines must be transported off-site at least monthly
- Backups of specific databases will be taken daily between the hours of 2 a.m. and 5 a.m. Locations of the databases will be provided in the POM.

eSig service requires high availability. This service will be made available to the constituency 24 hours a day, 7 days a week. The system stores the signature keys for users when the criticality of the system is also high. The eSig solution ARX CoSign supports high availability which provides redundancy and load balancing between multiple instances.

2.5.7. Single Sign-on Requirement

The eSig service is not available to the general VA public; use of this service requires successful authentication through the SSOe authentication process.

2.5.8. Requirement for Use of Enterprise Portals

eSig is a system to system web service thus this section is Not Applicable.

2.5.9. Special Device Requirements

- Special requirements for this device are entailed in the government requirement for cryptography to be FIPS 140-2 compliant.
- ARX Cosign is a special device used to support eSig.

2.6. Legacy System Retirement

There is no legacy eSig system that requires undergoing closure/retirement activities.

3. Conceptual Design

This section of the SDD provides details about the following topics:

- Conceptual Application Design
- Conceptual Data Design
- Conceptual Infrastructure Design

3.1. Conceptual Application Design

This section provides the conceptual design of the eSig solution.

3.1.1. Application Context

This section provides context for Electronic Signature (eSig) and its relationship to AcS.

Figure 6 below depicts the high-level interactions between eSig and the various activities, including interactions between AcS, with other VA applications, and to internal/external business partner applications.

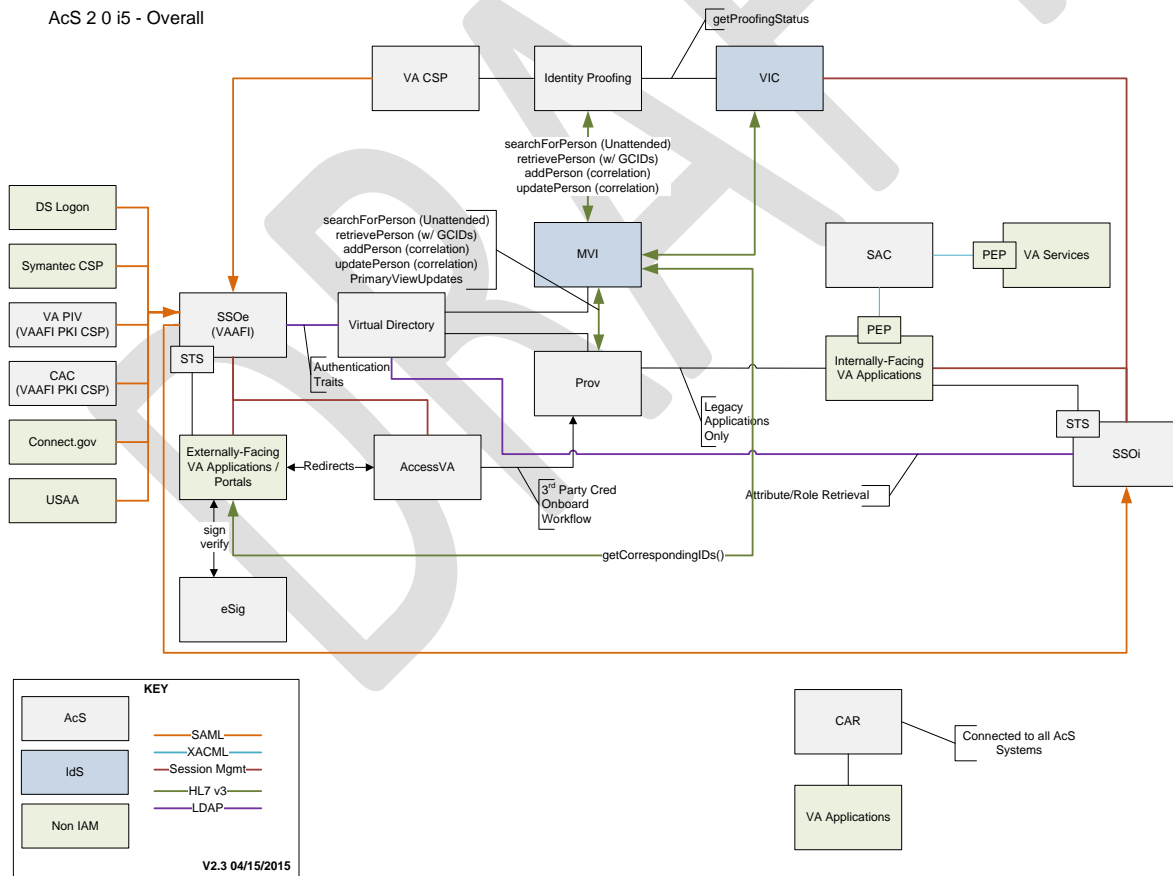


Figure 2: AcS 2.0 Application Design

The following table provides high-level description for each of the AcS activities. The external interfaces are interfaces for systems outside of VA and internal interfaces are interfaces for systems within VA.

Table 11: Activities in the High-Level Application Design

ID	Name	Description	Service or Legacy Code	External Interface Name	Internal Interface Name
1	CSP	CSP provides external user's credentials to VA applications that are not eligible for another VA approved credential.	Service	Self Service and Registration	SSOE, IP, CAR
2	IP	IP facilitates evaluating and validating a user's identity to be true and unique to the degree (level) of confidence required by VA.	Service	N/A	MVI, CSP, CAR
3	eSig	eSig provides the ability to sign documents electronically.	Service	N/A	CAR
4	SAC	SAC provides the ability to maintain and process granular access decisions based on a set of business rules and user attributes.	Service	N/A	CAR
5	Provisioning	Provisioning associates an identity to one or more application accounts and the associated entitlements to the identity. Provisioning also provides the capabilities for managing roles and certifying entitlements.	Service	TMS	AD, CAR, EDR, MVI, PIV, VDS, IP
6	SSOi	SSOi provides the desktop sign-on capability to internal VA users. SSOi also provides authentication and access to VA business applications for both internal and external user populations. External credentials are brokered by the SSOE service and are a federated partner with SSOi.	Service	Federation	AD, IP, CSP, Provisioning, SAC

ID	Name	Description	Service or Legacy Code	External Interface Name	Internal Interface Name
7	CAR	CAR provides the ability to proactively monitor, mitigate, and recover from potential compliance infractions and incidents.	Service	N/A	SSOi, Provisioning, CSP, IP, eSig, SAC

The eSig solution activities is described in greater detail below.

3.1.1.1. eSignature

The eSig service interfaces with the SSOe system via a webservice. The SSOe AuthN service employs Service Oriented Architecture (SOA) based principles to communicate with the eSig service. The ARX CoSign is a server-based digital signature solution that provides electronic signing capabilities to all of the authorized users connected through the network.



Figure 3: eSig Service Context

Table 12: Application Context Description

Interfaces Internal to Office of Information and Technology (OIT)					
ID	Interface Name	Related Object	Input Messages	Output Messages	Other CBP Party
1	SSOe	eSig	Election to sign a document with authorized access to SSOE	Signed document	IAM

3.1.2. High-Level Application Design

The high level Design below demonstrates that the eSig architecture is composed of the ARX Co-sign Digital Signature Device.

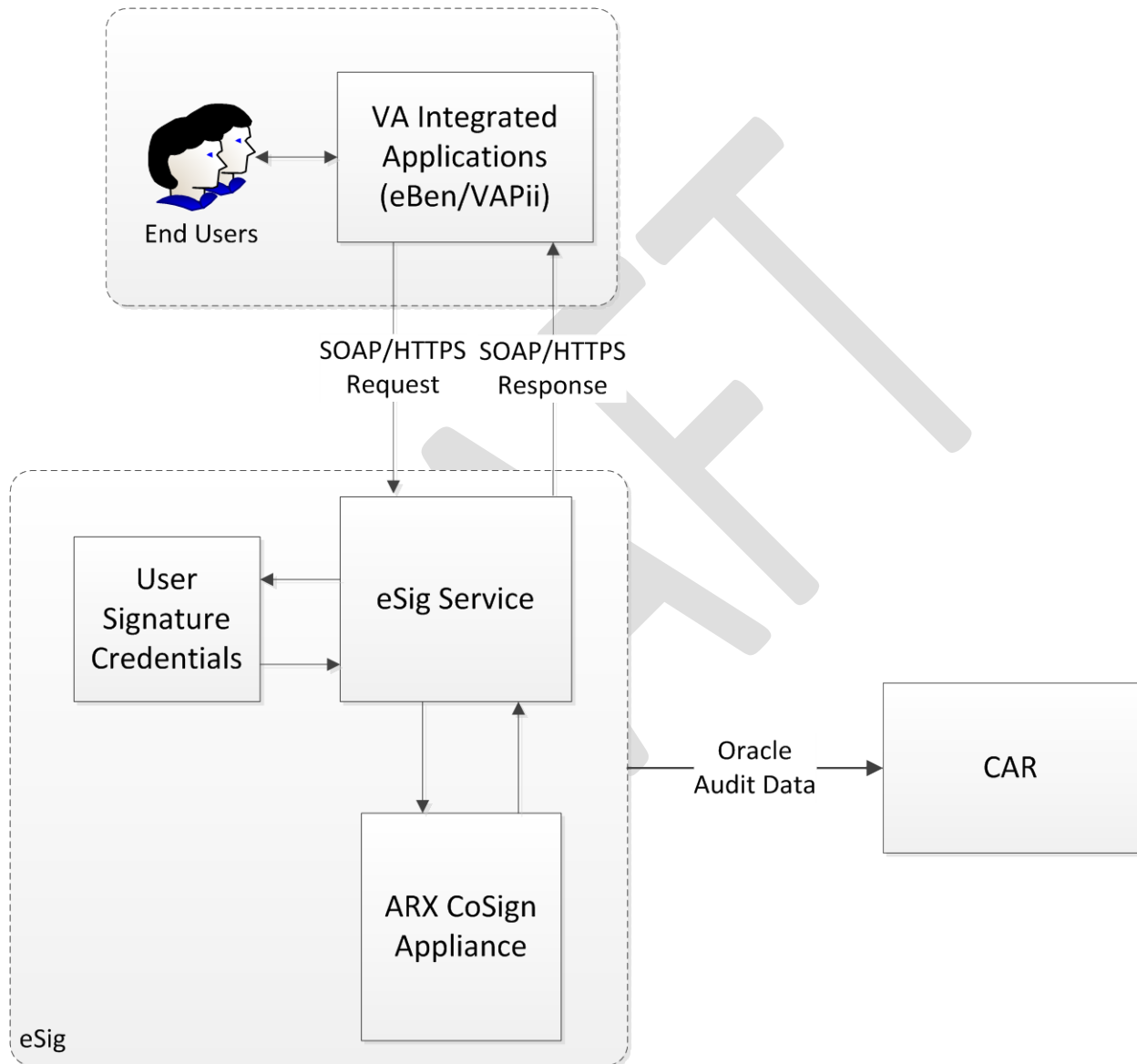


Figure 4: eSig High Level Design

Table 13: Objects in the High Level Application Design

Objects								
Name	ID	Description	Service or Legacy Code	External Interface Name	External Interface ID	Internal Interface Name	Internal Interface ID	Service Directed Projects (SDP) Sections 1&2
eSig	1	Performs electronic signature of documents	Service	None	None	VAAFISSOE	1	N/A
CAR	2	Provides Reporting	Service	None	None	CAR	2	N/A
End Users via eBen/VAPii	3	Integrated application	Service	N/A	N/A	eBen/VAPii	3	N/A

3.1.3. Application Locations

The following table lists the application components and their locations where they will be hosted.

Table 14: eSig Application Locations

Application Component	Description	Location at Which Component is Run	Type
ARX CoSign Device	Stores the Key pair for the eSig Service.	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)	Business Logic

Application Users

Application Component	Location	User
ARX Co-Sign	AITC	Approved VAAFI users

3.2. Conceptual Data Design

The following sections provide the conceptual data design for the AcS 2.0.

3.2.1. Project Conceptual Data Model

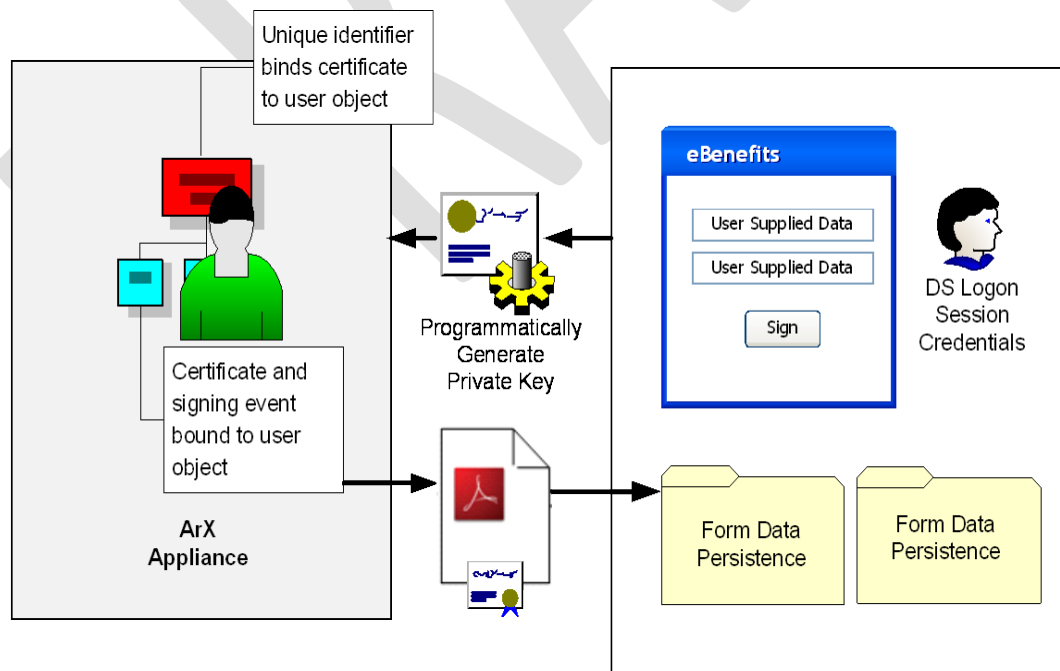


Figure 5: eSig Project Conceptual Data Model

This section describes the conceptual data model providing high-level representation of the data entities and relationships. The data objects within the AcS 2.0 eSig, how they are used, and how they relate to each other are provided in the Figure above.



Data Model
Elements - SDD emb

Database Information

The selected solution, CoSign ARX, will obtain user information via a web service call. Additionally, the CoSign ARX solution is comprised of its own database for key storage.

Table 15: Database Inventory

Database Name	Description	Type	Steward
ESIGDS	eSig DB	JDBC Data Source	N/A

The DB connection information from WebLogic to support eSig is:



DB INSTANCE	SCHEMA / Username
ascdb	ESIG

3.2.2. Database Information

N/A

3.2.3. User Interface Data Mapping

This section describes and defines the data that will be available for users of the eSig solution via the user interfaces and stored/retrieved from the database, if applicable.

Out-of-the-box screens are not shown.

3.2.3.1. Application Screen Interface

Refer to SSOe SDD, Section 6.4.9 for application screen references to support the eSig attestation page.

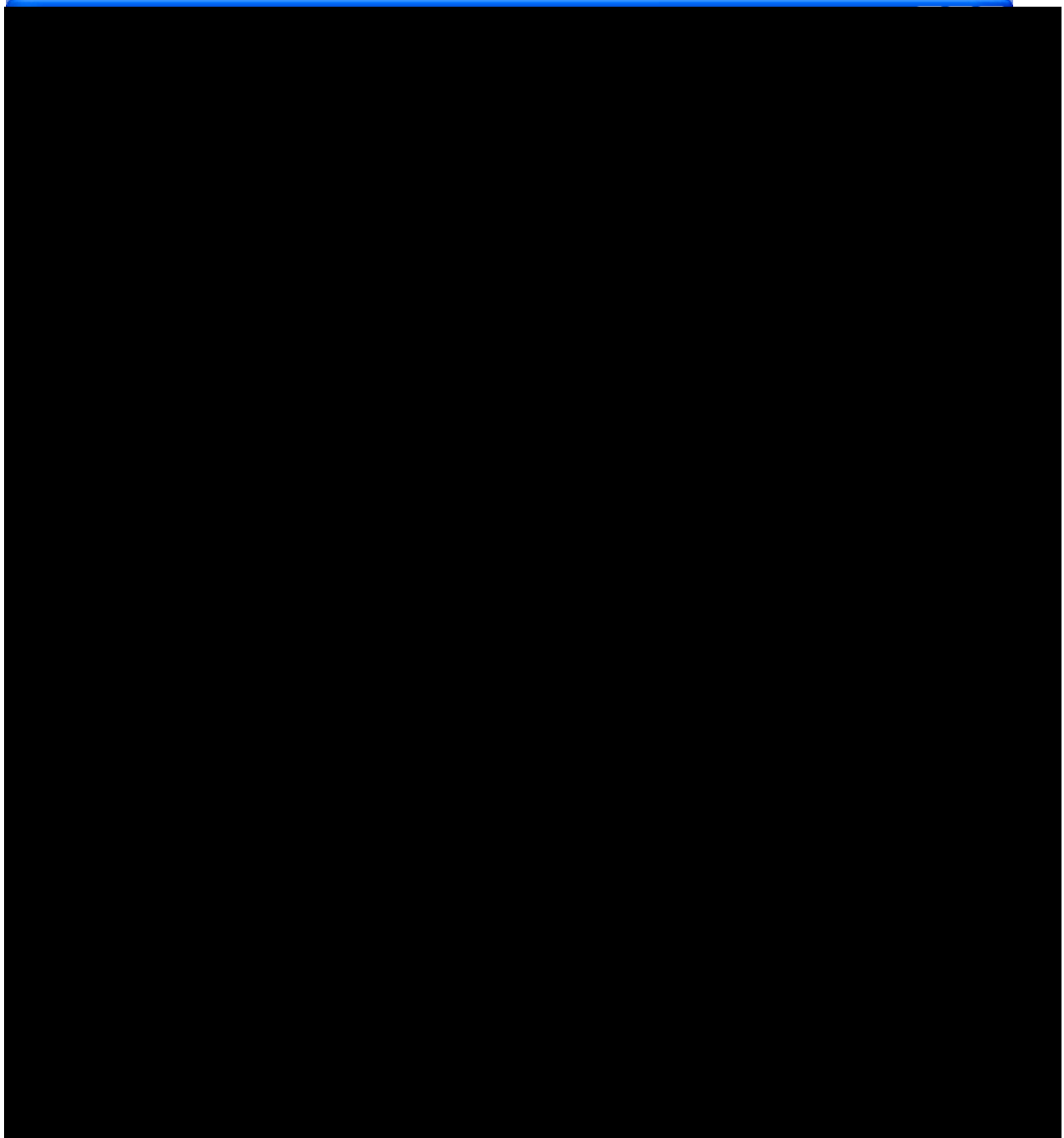


Figure 8: CoSign CA Certificate

3.2.3.2. Application Report Interface

eSig is integrated with the CAR solution. Please refer to the CAR SDD for further details.

3.2.3.3. Unmapped Data Element

N/A

3.3. Conceptual Infrastructure Design

The section provides a conceptual design of the infrastructure needed for the core capabilities of eSig. The section focuses on the primary environments and locations where the eSig is installed. The information is provided as preliminary design and is elaborated in later detailed design section.

The eSig device is shown below:

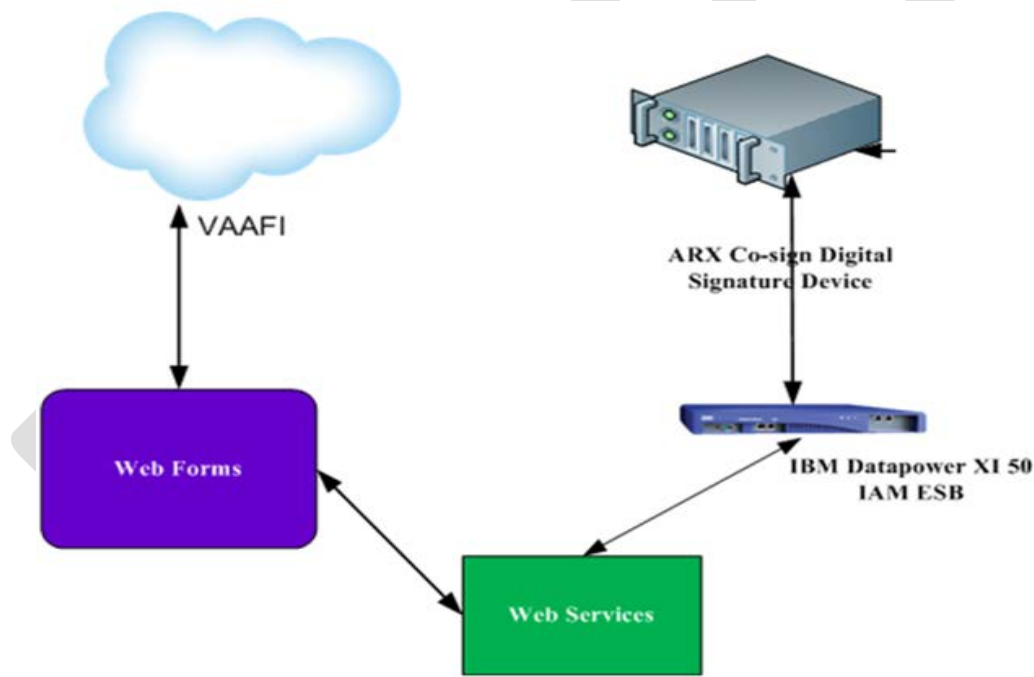


Figure 9: High Level Infrastructure Design

3.3.1. System Criticality and High Availability

The VA AcS infrastructure supports critical business systems. The current availability requirement for mission critical systems is 99.9%. The current data centers support 99.6% availability. The Production, Preproduction, and Disaster Recovery (DR) Data Center is hosted by Terremark in Culpeper, Virginia and Miami, Florida. Terremark does not currently support an active/active geographic failover and load balancing thus failover to the DR site could take

between one (1) and eight (8) hours. To mitigate the risk of not having a complete site failover, the AcS production infrastructure is intended to be scalable with limited single points of failure.

The DR site is contingency site that will resume data center operations in the event of a site failure. Load balancing, fault tolerance, backups and archiving, is a function of the hosting facility, Terremark and the data center operations team. Backups are described more fully in the Production Operations Manual (POM), but essentially are the following:

- Full backups are taken of virtual machines on a weekly basis
- Backups of virtual machines must be transported off-site at least monthly
- Backups of specific databases will be taken daily between the hours of 2 a.m. and 5 a.m. Locations of the databases will be provided in the POM.

The eSig prototype uses a hardware-based digital signature device which can be clustered to support high availability and eliminate single point of failure.

3.3.2. Special Technology

The following table provides information about the special technologies implemented as part of the AcS 2.0.

Table 16: Special Technology Requirements

Special Technology	Description	Notional Location	TRM Status
WebSphere DataPower XI50	DataPower provides the needed WebService capabilities to SSOE and to AcS.	Terremark	Yes
ARX Co-Sign (eSig)	Provides a PKI-based solution for digital signing documents, forms, and transactions.	Terremark	Yes

3.3.3. Technology Locations

Refer to section 3.3.4.1 below for technology locations.

3.3.4. Conceptual Infrastructure Diagram

This section depicts the AcS 2.0 with many of its internal and external connections exposed. Each sub-system of the infrastructure will be described in the next sections of this document. In each section, these connections will be described and an internal breakdown of the components will also be shown.

3.3.4.1. Location of Environments and External Interfaces

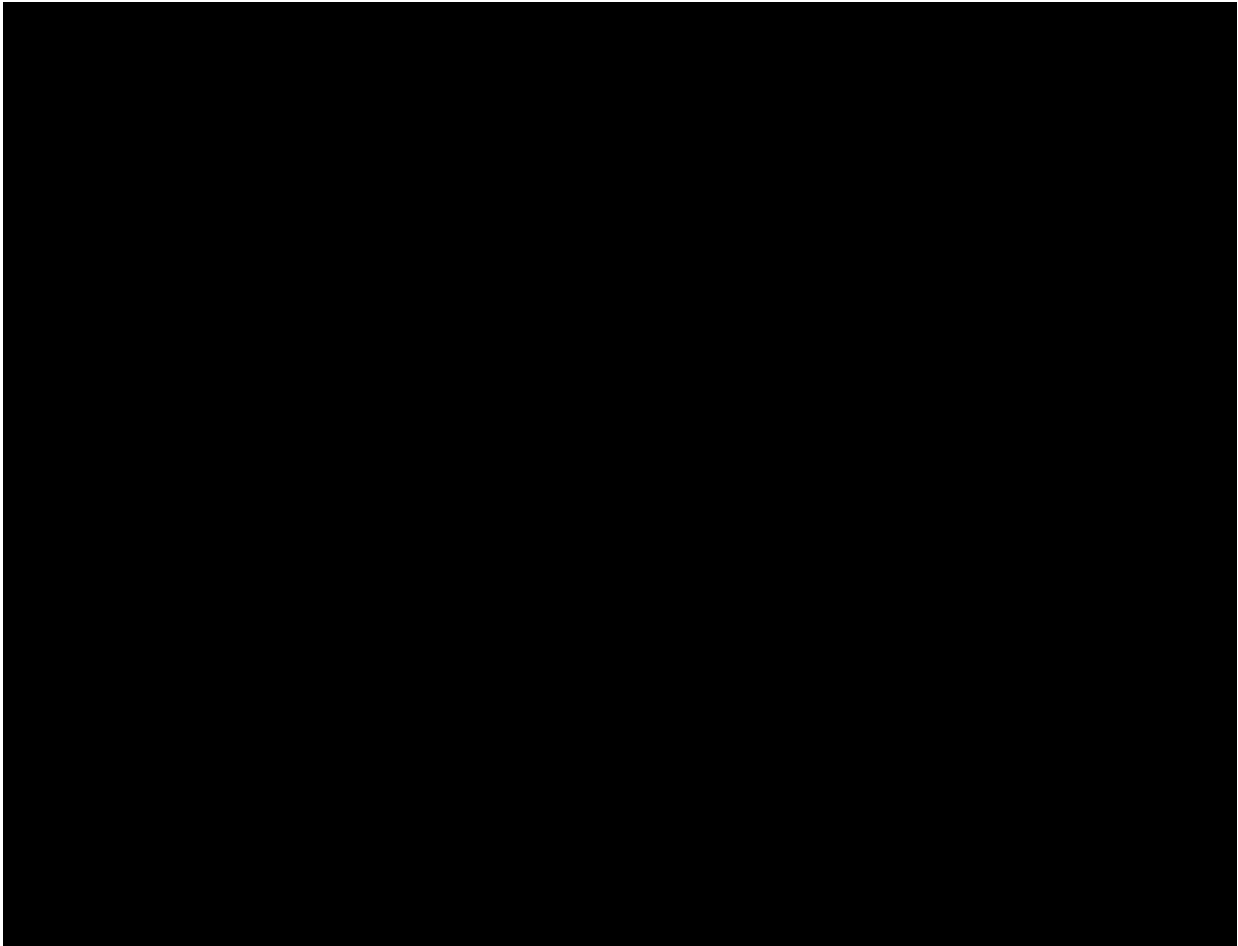


Figure 10: Conceptual Networks and Environments

Development Environment (DEV) AITC – Austin, TX

- This environment is utilized by the Development team for initial development of service enhancements, integrations with consuming applications, defect resolution, and unit testing.
- This is a loosely controlled environment for the AcS developers to use. The development team implements and maintains the COTS products, COTS patches, and code.
- System administrators maintain the operating systems and operating system patches.
- Code and configuration is stored in Subversion source control and exported as a build when moving to the next environment.
- The initial setup instructions are fine-tuned; the migration instructions are provided to migrate the code and configuration to the subsequent environments.

Software Quality Assurance (SQA) AITC – Austin, TX

- This environment is utilized by the Development team for integration testing, load, configuration, and quality tests.
- System Administrators install, configure, and operate applications as testing is performed.
- This is a tightly controlled environment and closely resembles the Production architecture. Issues with performance or the setup instructions are performed between Developers and the Administrators responsible for the environment.
- The setup instructions are fine-tuned.

Pre-Production – Terremark Culpeper, VA

- The User Acceptance Test (UAT) for the AcS is performed in this environment.
- This is where performance testing occurs.
- System Administrators install, configure, and operate applications per the fine-tuned setup instructions and provide support as testing is performed.
- Any remaining issues with performance or the setup instructions are worked out with the System Administrators.
- The setup instructions are finalized.
- This is a tightly controlled environment and is as close to identical as possible to the Production environment.

Production – Terremark Culpeper, VA

- The finalized setup instructions are installed.
- The environment is closely monitored.

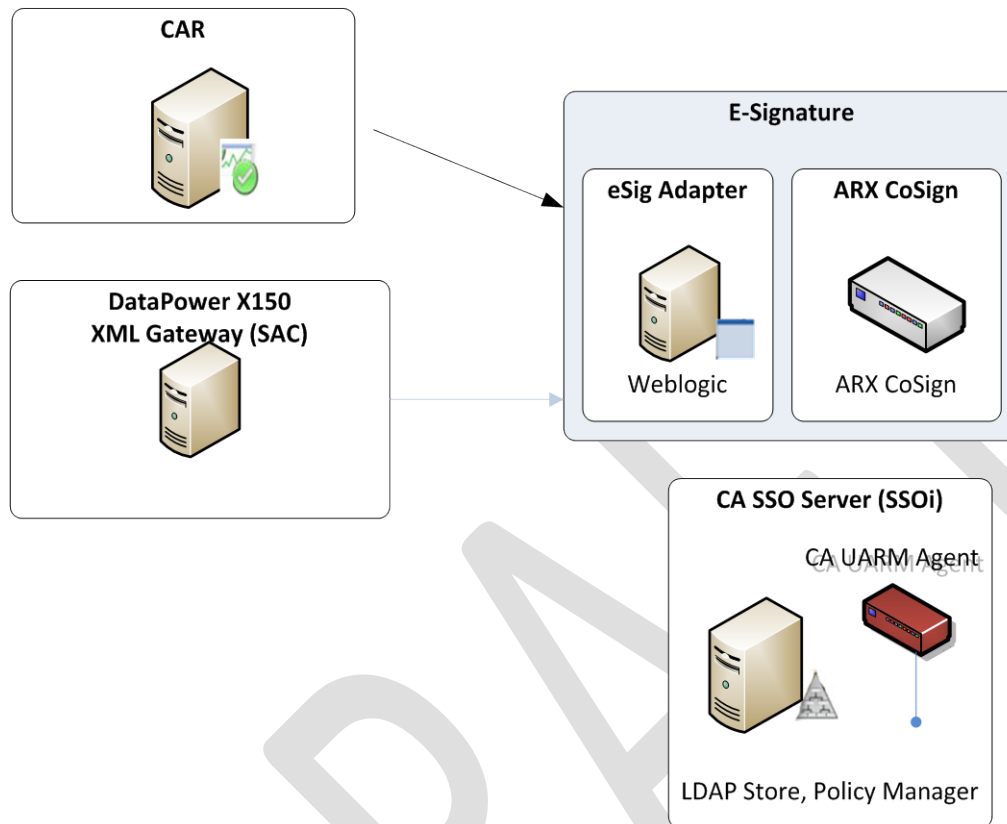
Production Disaster Recovery (DR) – Terremark Miami, FL

- This site provides hot failover capability so that services and data are maintained in the event of a failure in Production.
- This environment is identical to the Production environment.
- Once the change to Production is verified, the change is implemented in the DR environment.
- The DR environment is in the Terremark Miami, FL data center. The environment is configured with an Active-Passive topology.

3.3.4.2. Conceptual Production String Diagram

The following diagram, Figure 11, provides a logical view of the eSig components.

Figure 11: Logical Network String Diagram



4. System Architecture

The AcS 2.0 system architecture includes the hardware, software, and communication architectures. The hardware architecture describes the physical components needed in the system and their relationship to one another. The software architecture describes the software products, components, and code needed to provide the AcS 2.0. The communication architecture describes the connection and security requirements needed between the hardware components.

4.1. Hardware Architecture

The following diagram, Figure 12, shows the eSig hardware architecture and network topology.

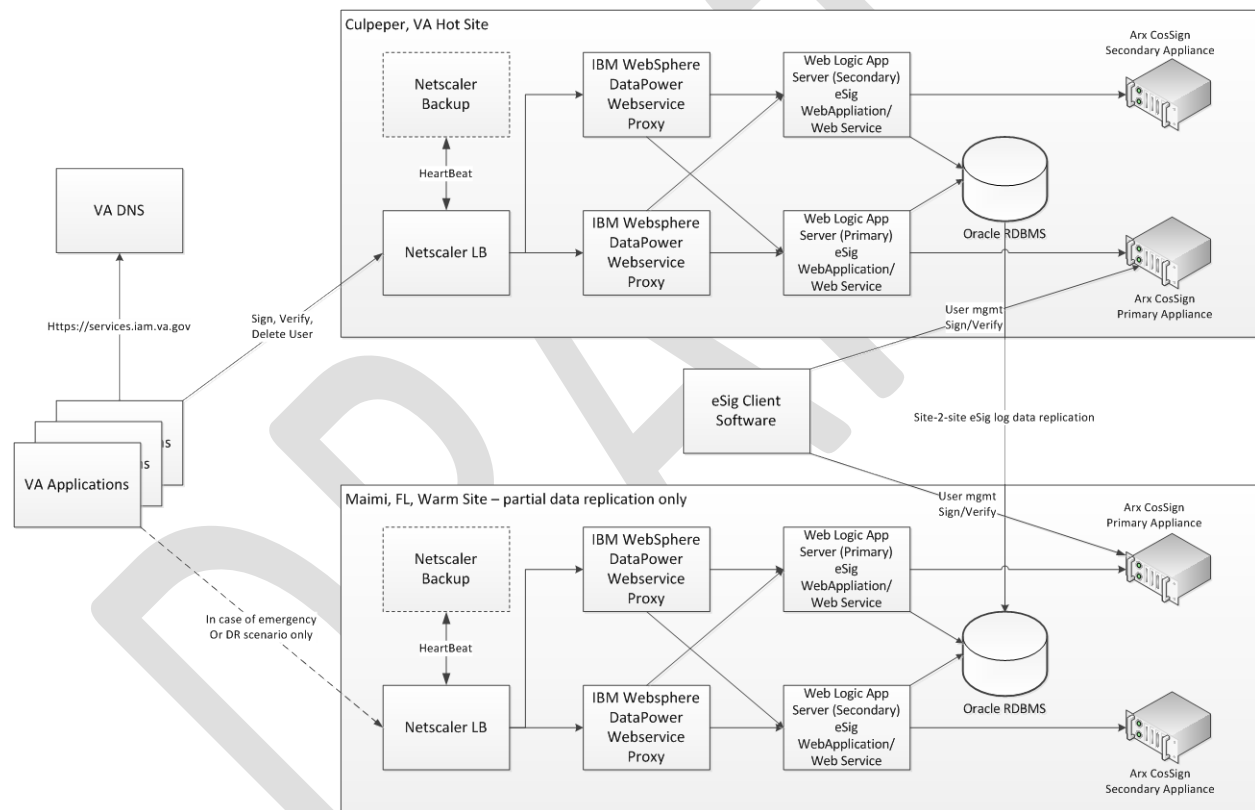


Figure 12: Network Communication Architecture

The following table provides information for the hardware appliances used for eSig.

Table 17: Hardware Appliance

Hardware Appliance	Descriptions	High Availability (HA)
ARX Co-Sign (eSig)	<p>The ARX CoSign appliance is a PKI-based, off-the-shelf digital-signature solution enabling VA to embed digital signatures in various documents, forms, and transactions. CoSign is a turnkey, hardware-based solution that is easily and quickly deployed in the network and provides cost-effective digital-signature capabilities for the organization. CoSign stores the signature credentials in a secure appliance, and maintains that the signer has exclusive access user's signature credentials, while still maintaining a centrally managed solution.</p>	<p>The ARX CoSign appliance has a built-in mechanism to provide High Availability configuration. eSig's HA setup uses two CoSign appliances. One is defined as the primary and the other is designated as the secondary cluster member. All information processed by the primary appliance is replicated securely to the secondary appliance using IPSEC protocol. In case of a replication failure, up to ten retries are made and if still unsuccessful, an alert is sent to the designated eSig administrator point of contact as configured on the appliance. The custom eSig webApplication under normal circumstances always communicates with the primary CoSign appliance. The communication is configurable through a property file -- the "eSigadapter.properties" file. In case of hardware problems and/or maintenance periods when the secondary appliance needs to be made the primary and vice-versa, a change in the eSig WebApplication property file is not necessary as the switching of the roles of the appliances, swaps their network configuration as well. Currently there is no replication between the eSig cluster information across physical sites - e.g. Production appliances in Terremark's Culpeper, VA Production site do not share information with their counterparts in the Miami, FL Disaster recovery site. Additional backup/restore procedures will be necessary to switch eSig to use a different physical site in case of emergency or actual disaster recovery.</p>
IBM DataPower	<p>A critical component of AcS infrastructure to securing web service message flows as a proxy using IBM DataPower Appliance</p>	<p>For High Availability configuration, the DataPower XI52 appliances will reside behind a Citrix Netscaler. This setup will have no effect on the existing DataPower configurations, as each transaction will be independent and processed separately by each DataPower appliance. The load balancer will serve as a reverse-proxy to distribute network traffic. The goal is to improve the overall burden of a single machine by enabling an industry standard algorithm.</p>

The uniform resource locators URLs eSig for production, pre-production and SQA are provided in the table below. The AcS components residing in the DMZ are the external facing web servers that contain the CSP pages and federation components. These components will be load balanced by the Citrix Netscalers located in the Terremark GSS. DataPower, along with the remaining AcS application components, will reside in the GSS. The following table provides details on the eSig machines such as ports, URLs, protocols hostnames for each application in every environment.

**Table 18: Virtual Machines and Appliances
SQA (AITC)**

Application	Number of VMs	Number of Physical Servers	Hostname
ARX CoSign (Appliance)	N/A	1	[REDACTED]
eSig WebLogic Servers Admin service on primary node	2	N/A	[REDACTED] [REDACTED]

Pre-Production (Terremark Culpeper, VA)

Application	Number of VMs	Number of Physical Servers	Hostname
ARX CoSign (Appliance)	N/A	1	[REDACTED]
eSig WebLogic Servers Admin service on primary node	2	N/A	[REDACTED] [REDACTED]

Production (Terremark Culpeper, VA)

Application	Number of VMs	Number of Physical Servers	Hostname
ARX CoSign (Appliance)	N/A	2	[REDACTED] [REDACTED]
eSig WebLogic Servers	2	N/A	[REDACTED] [REDACTED]

DR (Terremark Miami, FL)

Application	Number of VMs	Number of Physical Servers	Hostname
ARX CoSign (Appliance)	N/A	N/A	N/A
eSig WebLogic Servers	2	N/A	[REDACTED]

4.2. Software Architecture

The following diagram shows the complete software architecture for SAC. (Will be updated on 04/20/2015 by Anand)

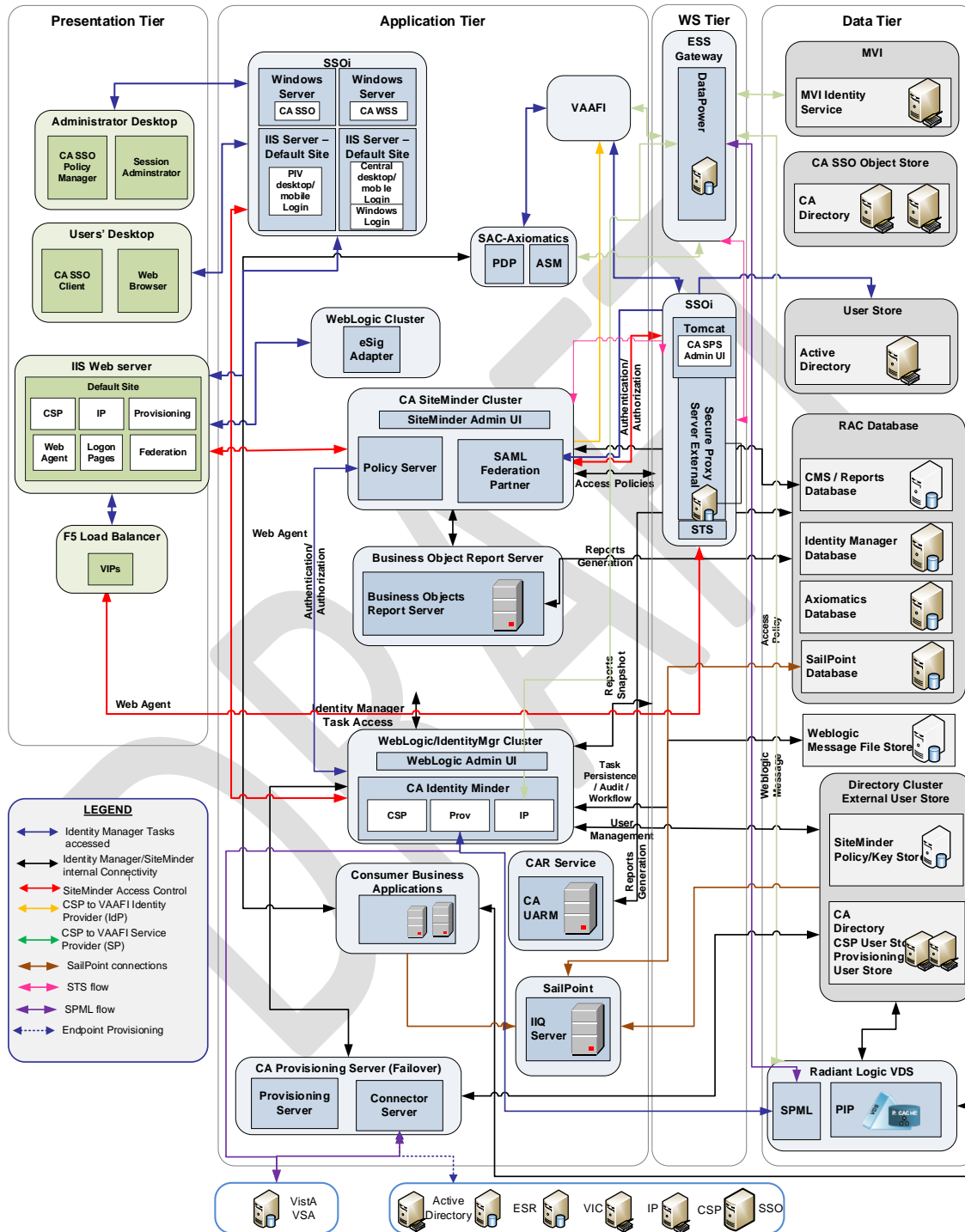


Figure 13: Software Architecture

The following table describes the eSig products and versions.

Table 19: eSig Products and Versions

Products	Abbreviation	Product Version/Release
ARX Co-Sign	Digital Signature	v6.3
WebLogic	-	10.3.6

The following table provides information about the software components.

**Table 20: Software Components
Oracle Database 11gR2**

The shared database environment will maintain the following table spaces required for the components of the AcS implementation. Database High Availability and Data Guard to synchronize and replicate a HOT Oracle database environment to Terremark Miami, FL.

Characteristic	Description
Database Table spaces	Data Table spaces: ESIGAUDIT_DATA, Users Temp Rollback Undo
High Availability	For the AcS 2.0, database high availability is critical. A database outage can cause a multitude of errors to occur on the application side, thereby nullifying the high availability configurations on the application itself. It was planned for Raw Devices to be utilized by Oracle Automatic Storage Management (ASM) file system, working as the volume manager, overseeing the clusterware file systems. ASM, attached by each node, exposes the existing pool of storage and makes it available as an interface for the Oracle database files. The ASM is supported by Oracle Clusterware. If a single Oracle instance on a node fails, the ASM and database instances on the surviving nodes are designed to automatically failover. Due to the load dependency on the ASM file system storage, mirroring is needed to provide high availability.

eSig Web Application

The eSig custom WebApplication is the isolation layer for the core eSig appliance, providing the client/partner exposed eSig functionality. eSig uses the CoSign appliance as a building block and provides the capability to digitally sign documents to applications within VA. All events, associated with each digital signing, verification or user deletion operations, are recorded and made available to the CAR service for reporting.

Characteristic	Description
----------------	-------------

Characteristic	Description
Subcomponents	<p>DataPower devices: The DataPower devices are used to authenticate the machine-to-machine sessions.</p> <p>WebLogic Server: The WebLogic Server hosts the eSig adapter. The eSig adapter has the following components:</p> <p>Java Web Application</p> <p>The eSig Web Application is a standard J2EE application utilizing a combination of MVC and Façade design patterns. The eSig servlet, part of the abbreviated MVC pattern, currently accepts only SOAP WebService calls but can be extended with a Web UI if required. The Façade pattern component carries out the following categories of operations:</p> <ul style="list-style-type: none"> ○ User Management: The user management function allows the service to add or remove aneSiguser. ○ Sign and Verify: This allows the applications to sign a given document. ○ Reporting Events: This category allows the eSig service to record events that will be reported via CAR service. <p>CoSign Appliance: The CoSign Appliance is a networked hardware device that stores the user certificates.</p>

Characteristic	Description
High Availability	<p>The DataPower appliances have an inherent, self-contained HA feature where the appliance will auto failover to the other appliance; however, the DataPower appliances do not support internal load balancing.</p> <p>WebLogic domains are created in clusters consisting of multiple WebLogic Server instances running simultaneously and working together to provide increased scalability and reliability. A cluster appears to clients to be a single WebLogic Server instance. The server instances eSig uses run on separate VMs (systems). The eSig WebApplication runs within an application server cluster and is highly available through multimode cluster and is load balanced by F5 (DEV/SQA) and by Citrix Netscaler (PREPROD/PROD) and DataPower.</p> <p>CoSign is highly available through internal functions that keep the appliances in sync with each other.</p> <p>The High availability feature within the ARX CoSign appliances requires a minimum of two CoSign appliances is configured for manual failover through switching of the roles of the current primary and secondary appliances. In case of failure of the primary CoSign appliance, the secondary is promoted to a primary and it takes over the eSig tasks. *** Active-Active load balancing of the requests among the two devices is not supported. Replication of the configuration and user data is ensured between the two devices, thus allowing for manually initiated failover with limited amount of downtime. The communication interface between the ARX CoSign WebLogic servers and the appliance(s) is through a DNS registered FQDN, pointing to an IP address, registered with the Primary appliance. At the time of the manual failover, the IP address configuration is also swapped, thus allowing for uninterrupted communication from the WebLogic App Server custom eSig component to the appliances.</p> <p>*** NOTE: Current status is Active-Active (Primary-Primary) configuration of the CoSign Appliances. Both appliances are on a nightly automated backup schedule leveraging a utility provided by ARX CoSign.</p>

The following table defines the programming languages used for development within the VA AcS 2.0.

Table 21: Programming Languages

Programming Languages	Definition/Description
Java	Java language was used to develop custom class/jar file for IdentityMinder Business Logic Task Handler BLTH.
XML	Common configurations are stored as XML files.
XACML	XML-based language for development of privileges/role management.
JavaScript	Scripting language.

4.3. Network Architecture

The following diagram depicts the communication channels between the different AcS components and protocols used. *(Will update with Port information)*

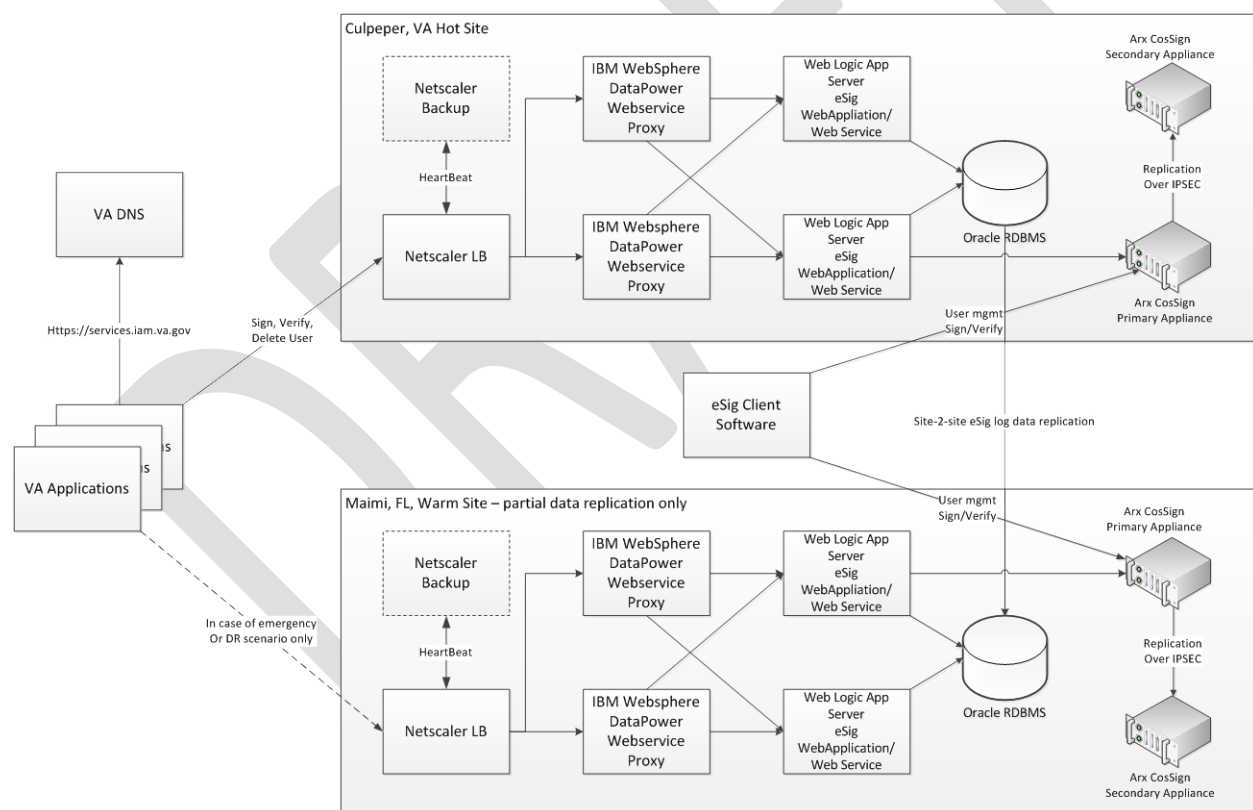


Figure 14: AcS Network Security Topology

Table 22: Network Architecture

Application	Network	Port(s)	Reason	Protocol(s)
ARX CoSign	Internal	████	API Calls	HTTPS
eSig WebLogic	Internal	████	Administration Port	HTTPS
eSig WebLogic	Internal	████	Manage Server Port	TCP
eSig WebLogic	Internal	████	Node Manager	TCP

4.4. Service Oriented Architecture/ESS

eSig provides authenticated users the ability to digitally sign an approved electronic document. Once the eSignature user is authenticated by the application integrated with the eSignature Service, the eSignature Service assumes that the authenticated user has a LOA 2 or higher credential. The integrated application then passes the user token and document to be signed to eSignature for signing.

eSig provides a Web Service interface enabling rapid integration for SOA based applications. ARX CoSign allows users to electronically sign documents, records, files, forms, and other electronic transactions. CoSign enables users to sign multiple document-format types (Word, PDF, and others) resulting in seamless user adoption.

The following web services are supported by eSig and further detailed within Section 6.4.

- Sign
- Verify
- Delete

4.5. Enterprise Architecture

Please refer to the COTS Product Roadmap on the [AcS TSPR](#) site.

5. Data Design

This section outlines the design of the database management system (DBMS) and non-DBMS files associated with the eSig solution as well as the data security implementation.

5.1.DBMS Files

Table 23: Database File System

Table Spaces	Data Files
ESIG_DATA	+ORADATA/acsdbs/datafile/eSig_data

5.2.Non-DBMS Files

N/A

5.3.Data View

N/A

6. Detailed Design

This section describes the design for the eSig solution and its activities in detail.

6.1. Hardware Detailed Design

The sections below provide the hardware information for each activity in eSig. The following table displays the sizing, network, Operating System, and number of Virtual Machines required to be deployed for eSig:



6.2. Software Detailed Design

This section provides final detailed information associated with the design of eSig solution activity and the associated functionality.

The VA business processes require that for many activities the nations Veterans, VA business partners and other persons of interest must provide signatures. The eSig activity provides the ability for users to submit a signature electronically when doing business electronically with VA.

6.2.1. Conceptual Design

This section introduces the conceptual information that establishes the basis for eSig is built.

6.2.1.1. Product Perspective

Refer to section 3.1.3 for information on COTS products for the AcS 2.0.

6.2.1.1.1. User Interfaces

Refer to section 3.2.3 for information on user interfaces.

6.2.1.1.2. Hardware Interfaces

Refer to section 6.1 for information on hardware configurations and interfaces.

6.2.1.1.3. Software Interfaces

Refer to section 4.2 for software architecture design for the eSig.

6.2.1.1.4. Communications Interfaces

The following table displays the necessary port communications and protocols used for each component-based server. The ports described must be open for both inbound and outbound communications. The ports mentioned below indicate inbound ports and are opened to AcS components for communication.

Table 24: Port Communications and Protocols

Application	Network	Port(s)	Reason	Protocol(s)
ARX CoSign	Internal	████	API Calls	HTTPS
eSig WebLogic	Internal	████	Administration Port	HTTPS
eSig WebLogic	Internal	████	Manage Server Port	TCP
eSig WebLogic	Internal	████	Node Manager	TCP

6.2.1.1.5. Memory Constraints

This section is not applicable to the eSig.

6.2.1.1.6. Special Operations

Refer to the eSig Configuration Guide and POM for eSig (backup special operations that is encompassed within these documents)



Production
Operations Manual

6.2.1.2. Product Features

The AcS 2.0 is based on the foundation of CA COTS products. The table below describes the AcS 2.0 products.

Table 25: AcS 2.0 Products

Software	Description
CA Directory	<p>CA Directory provides directory services and security for online applications for organizations. For example, it enables customers to access their electronic accounts; employees can access critical business data.</p> <p>This product is generally considered a highly scalable and distributable implementation of directory services, including security services (e.g., authentication).</p> <p>CA Directory is supported on a variety of Windows and UNIX platforms, as well as 64-bit operating systems such as Linux 64, Solaris 10/Intel 64, UltraSparc 64, IBM Power5 64 and HP-UX Itanium 64.</p> <p>CA Directory supports open standards including: LDAP (and related RFCs), X.500 (DAP, DSP, DISP), Security (SSL, TLS, password hashes), Management (SNMP and related RFCs), Network (IPv6, RFC1006), and US Federal Government standards (FIPS 140-2, Common Criteria EAL3, and Section 508).</p>

Software	Description
Axiomatics	The Axiomatics Policy Server (APS) is a powerful access control system that allows users to manage, simulate and enforce fine-grained policies written in the eXtensible Access Control Markup Language (XACML). The Axiomatics Policy Server (APS) provides a full-fledged, XACML-based authorization service. The components are managed from a central point, the Axiomatics Services Manager (ASM).

6.2.1.3. User Characteristics

Refer to section 1.5 for user-related information.

6.2.1.4. Dependencies and Constraints

Refer to section 1.4 and section 2.4 for eSig constraints and dependencies.

6.2.1.5. eSig Design

The following diagram provides a detailed view of the complete eSig system at VA and its interaction with various systems and actors.

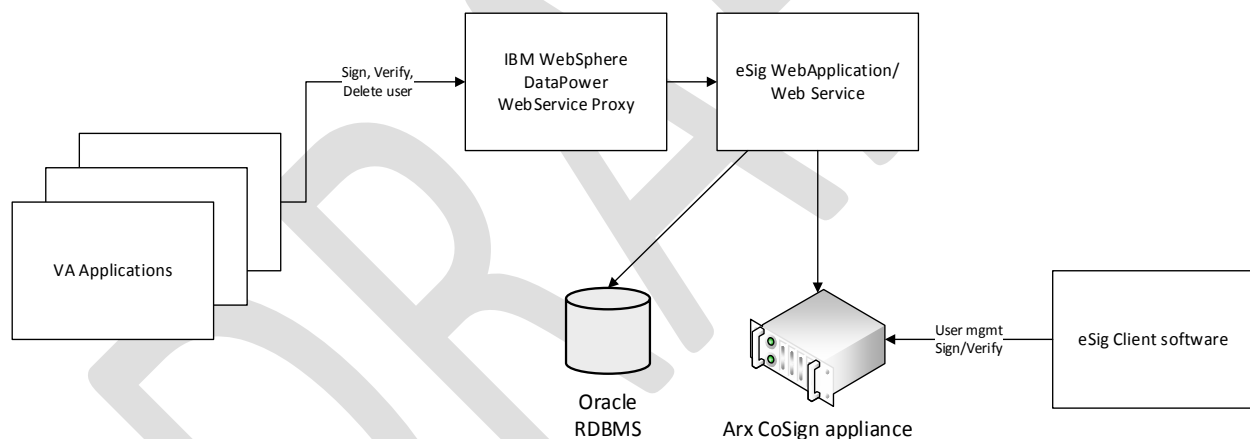


Figure 15: eSig Logical Design

The eSig custom code is implemented as Java/J2EE application, exposing a WebService interface. The implementation uses the Java Servlet API v2.3. This configuration allows integration of the eSig services with both web based applications and supports machine to machine SOAP WebService calls. The eSig WebApplication utilizes the façade design pattern, which allows for flexibility in backing interface definitions and abstraction from exposing backend system complexities to the eSig clients/partners. With the façade approach, any changes to the CoSign appliance will most likely not result in any changes on the eSig interface exposed to its clients/partners. The façade pattern allows for flexible manipulation of user roles and can prevent certain function calls based on the eSig request submitter's role. Requests to the eSig WebApplication are stateless. Parallel execution of the façade pattern implementation classes

(supported OOB by the underlying Web application server J2EE Web Container) allows for optimized scalability of the custom code.

The request from the end application is completely decoupled from the CoSign appliance and hence more controls can be built before the request reaches the CoSign appliance. This is imperative because the CoSign appliance has no access control list and no security inherent capabilities other than the password for the public private key pair. The functionality is similar to the Chain of Responsibility pattern but façade pattern is preferred for other reasons listed above.

Visible Signature:

The visible signature will include the signer's common name on the left side of the signature box, followed by the common name, with the email address under the common name (if supplied). The reason (if supplied) will be under the email address, and the signature date and time with the GMT offset value positioned under the reason on the right side of the signature box, as the following figure illustrates.



Figure 16: Example of a Visible Signature

6.2.1.5.1. Sign a Document

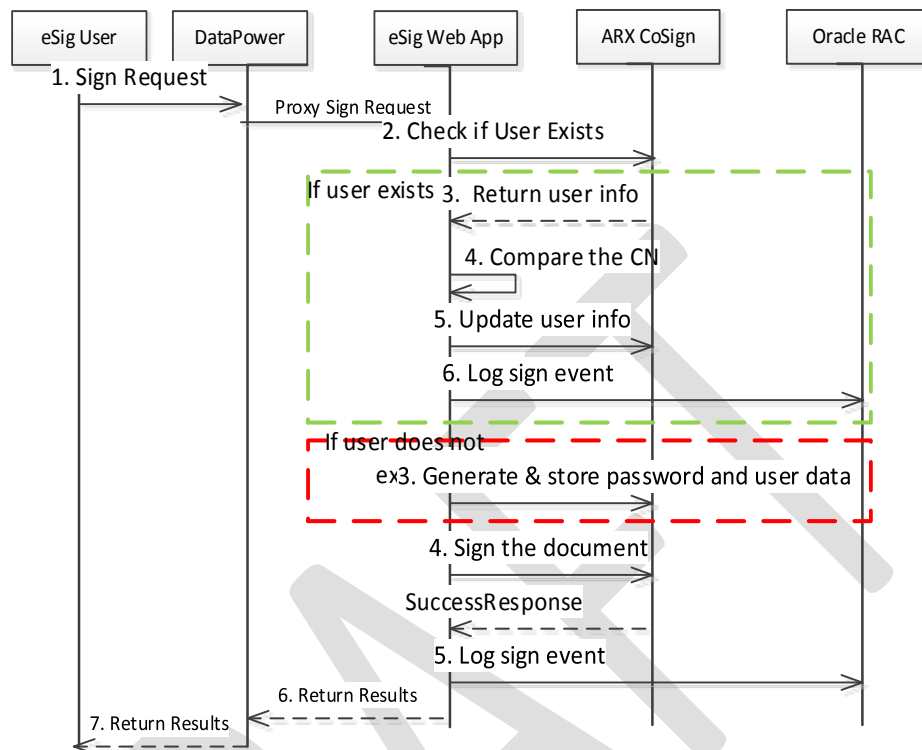


Figure 17: Sign a Document Sequence Diagram

Table 26: Sign a Document

Field	Description
Use Case Name	Sign a Document
Description	This Use Case describes the process through which a User signs a document electronically.
Actors	<ol style="list-style-type: none"> 1. eSig user 2. DataPower 3. eSig Web App (eSig Web Service) 4. ARX CoSign 5. Oracle RAC
Pre-Conditions	<ul style="list-style-type: none"> • The document type to be submitted is one of the supported types by eSig. • End user is authenticated with at least LOA 2 or above credential.

Field	Description
Trigger	A VA application sends a digital signing request to eSig.
Actions	<ol style="list-style-type: none"> 1. DataPower intercepts the signature request from the user and sends it to the eSig Web Service. 2. Upon receipt, the ARX CoSign device checks to see whether the user exists. 3. If the user exists: <ol style="list-style-type: none"> 3.1 ARC CoSign returns the user information 3.2 The eSig Web Service compares the CN 3.3 The eSig Web Service updates the user information in the ARX CoSign 3.4 The eSig Web Service logs the sign event with the Oracle RAC 4. If the user does not exist, eSig Web Service generates and stores the encrypted password and user data. 5. The eSig Web Service signs the document and sends the success response to ARX CoSign. 6. The eSig Web Service logs the sign event and returns results to DataPower.
Main Success Scenarios	The electronic signature succeeds and is captured on the document.
Main Failure Scenarios	The electronic signature fails and is not captured on the document.

6.2.1.5.2. Verify a Signed Document

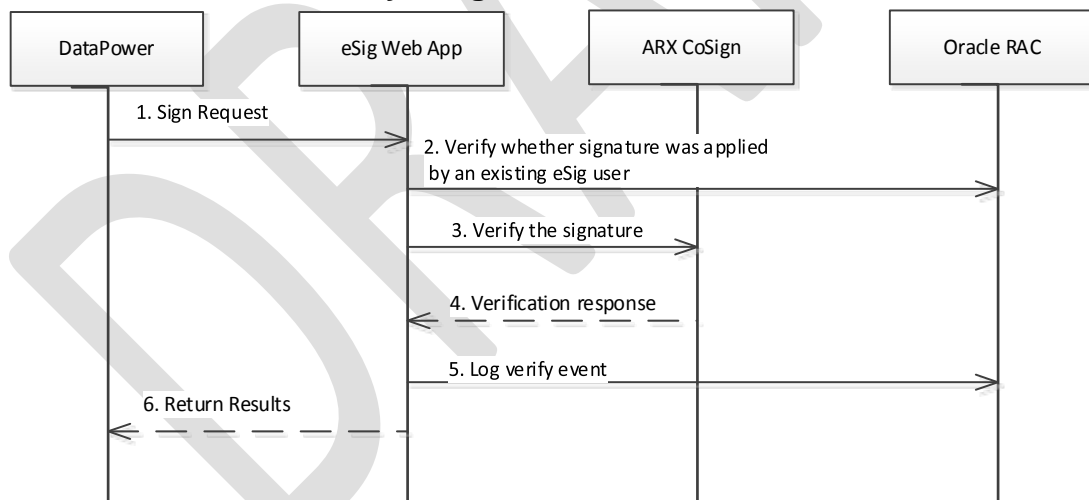


Figure 18: Verify a Signed Document – Sequence Diagram

Table 27: Verify a Signed Document

Field	Description
Use Case Name	Verify a Signed Document
Description	This Use Case describes the process through which a signed document is verified
Actors	<ol style="list-style-type: none"> 1. eSig user 2. DataPower 3. eSig Web Application (Web Service) 4. ARX CoSign 5. Oracle RAC
Pre-Conditions	The document type to be submitted is one of the supported types by eSig
Trigger	An already signed document is presented for verification.
Actions	<ol style="list-style-type: none"> 1. DataPower intercepts a request to validate a signature and sends it to the eSig Web Service. 2. Upon receipt, the ARX CoSign device checks to see whether the user exists. 3. The eSig Adapter verifies the signature against the ARX CoSign data 4. ARX CoSign verifies the signature 5. The eSig Adapter logs the verify event with the Oracle RAC 6. The eSig Adapters returns success to DataPower.
Main Success Scenarios	The electronic signature is verified and response is sent to requestor.
Main Failure Scenarios	The electronic signature is not valid.

6.2.2. Specific Requirements

The Design meets the business requirements provided in requirements documents listed in section 1.4.

6.2.2.1. Database Repository

N/A

6.2.2.2. System Features

N/A

6.2.2.3. Design Element Tables

N/A

6.2.2.3.1. Routines (Entry Points)

N/A

6.2.2.3.2. Templates

N/A

N/A	6.2.2.3.3. Bulletins
N/A	6.2.2.3.4. Data Entries Affected by the Design
N/A	6.2.2.3.5. Unique Record(s)
N/A	6.2.2.3.6. File or Global Size Changes
N/A	6.2.2.3.7. Mail Groups
N/A	6.2.2.3.8. Security Keys
N/A	6.2.2.3.9. Options
N/A	6.2.2.3.10. Protocols
N/A	6.2.2.3.11. Remote Procedure Call (RPC)
N/A	6.2.2.3.12. Constants Defined in Interface
N/A	6.2.2.3.13. Variables Defined in Interface
N/A	6.2.2.3.14. Types Defined in Interface
N/A	6.2.2.3.15. GUI
N/A	6.2.2.3.16. GUI Classes
N/A	6.2.2.3.17. Current Form
N/A	6.2.2.3.18. Modified Form
N/A	6.2.2.3.19. Components on Form

N/A	6.2.2.3.20. Events
N/A	6.2.2.3.21. Methods
N/A	6.2.2.3.22. Special References
N/A	6.2.2.3.23. Class Events
N/A	6.2.2.3.24. Class Methods
N/A	6.2.2.3.25. Class Properties
N/A	6.2.2.3.26. Uses Clause
N/A	6.2.2.3.27. Forms
N/A	6.2.2.3.28. Functions
N/A	6.2.2.3.29. Dialog
N/A	6.2.2.3.30. Help Frame
N/A	6.2.2.3.31. HL7 Application Parameter
N/A	6.2.2.3.32. HL7 Logical Link
N/A	6.2.2.3.33. COTS Interface

6.2.3. System Maintenance Design

During periods of system maintenance or outages, customer/user facing Graphical User Interfaces (GUI) have to be updated to inform the specific eSig audience of the state of the system, what the expected return to service timeframe is and any additional references (e.g., help desk numbers, ANR information) that may be needed for the users of the system in order to allow them to either use an out-of-band process or be kept informed of any progress as needed.

6.2.3.1. Maintenance Pages

eSig does not have a UI and therefore does not have a maintenance page.

6.3. Network Detailed Design

N/A

6.4. Service Oriented Architecture/ESS Detailed Design

This section details the following web services provided by eSig:

- Sign
- Verify
- Delete

The eSig interface is system to system only. Upon authentication, if a user does not exist in eSig, eSig will create an account with the user ID passed from the consuming application. eSig shall auto-create a password (although password is required, the user is never challenged for it).

6.4.1. Service Description for eSig

N/A

6.4.2. Service Design for eSig

N/A

6.4.2.1. Introduction

6.4.2.1.1. Purpose and Scope of Service

N/A

6.4.2.1.1. Links to Other Documents

N/A

6.4.2.2. Service Details

6.4.2.2.1. Service Identification

N/A

6.4.2.2.2. Service Versions

N/A

6.4.2.2.3. Summary of Design and Platform Details

6.4.2.2.3.1. SOA Pattern(s) Implemented

N/A

6.4.2.2.3.2. COTS Platform vendor names and versions for hosting platform

N/A

6.4.2.3. Dependencies

N/A

6.4.2.4. Service Design Details

N/A

6.4.2.4.1. Interface Technical Specs

N/A

6.4.2.4.1.1. Service Invocation Type

N/A

6.4.2.4.1.2. Service Interface Type

N/A

6.4.2.4.1.3. Service Name

N/A

6.4.2.4.1.4. Interface

N/A

6.4.2.4.1.5. End Points

N/A

6.4.2.4.1.6. Operations or Methods

N/A

6.4.2.4.1.7. Message Schemas

N/A

6.4.2.4.2. Information Model

N/A

6.4.2.4.2.1. Class Diagram and Description of Entities Involved

N/A

6.4.2.4.2.2. Mappings from ELDM to Standards Based Schemas

N/A

6.4.2.4.3. Behavior Model (AKA Use Case Realization)

N/A

6.4.2.4.3.1. Use Cases (Use Case Model)

N/A

6.4.2.4.3.2. Interaction Diagrams

N/A

6.4.2.5. Gap Analysis

N/A

6.4.2.5.1. Variances from Enterprise Target Architecture

N/A

6.4.2.5.2. Variances from SLDs

N/A

6.4.2.5.3. Variances from Standards and Policies

N/A

6.4.2.5.4. Justification for Exceptions and Mitigation

N/A

6.4.3. Sign

The eSig Service receives an authenticated/authorized electronic document signing request. The eSig service checks the validity of the request using the following criteria:

- The document signing request comes from a trusted VA application.
- The document sent for signing is in the list of acceptable types (e.g. Adobe PDF, MS Word, and web based forms).
- All necessary data, to perform the digital signing is sent with the request to eSig Service.

The eSig Service receives confirmation about user registration. If the eSig User is not registered, eSig shall add the user. The eSig Service compares the name on the existing user record in the eSignature data store to the name passed for the current document signing request. The eSig service retrieves the eSig user's PKI credential for the document signing process from the eSig User Store. The eSig service prepares the digital signature format to be applied to the submitted document (size, visibility, visual content, structure and placement of the signature). The eSig Service creates the signature on the submitted document using the eSig User's PKI credential. The eSig service returns the signed document to the requesting VA application.

The following links provide examples of the Sign Service:



SOAP_Sign_Reques
t.xml



SOAP_Sign_Respon
se.xml

6.4.4. Verify

The signature can be verified by opening the document and confirming the presence of the signature. The eSig Service receives a request to validate a digital signature on an electronic document. The eSig Service validates user is registered in eSig. The eSig Service retrieves the eSig User's PKI credential from the eSig User Store. The eSig Service validates the electronic document's digital signature with the eSig User's credential. eSig will then send out a notification to the VA application indicating digital signature validation status.

The following links provide examples of the Verify Service:



SOAP_Verify_Reque
st.xml



SOAP_Verify_Respo
nse.xml

6.4.5. Delete

This eSig Service upon request to remove an eSig User account and upon attaining confirmation about user registration. If the eSig User is registered, eSign shall remove the user account from the eSig User store. If the eSig User is not registered send notification of unsuccessful removal back to the VA application. eSig then provides a notification is sent to the VA application indicating eSig User account removal status.

The following links provide examples of the Delete Service



SOAP_Delete_Requ
est.xml



SOAP_Delete_Respo
nse.xml

Please refer to the eSig WSDL for detailed information on SOA/ESS design details.



ESigDSSService.wsd
l.xml

7. External System Interface Design

N/A

7.1.Interface Architecture

Refer to SSOE SDD for eSig attestation related information.

7.2.Interface Detailed Design

N/A

DRAFT

8. Human-Machine Interface

There are no end user UI for eSig. Admin UI information can be found within the [Training guides](#) and configuration guides for eSignature.

Refer to section 3.2.3, which provides the interfaces that are used by AcS activities as appropriate for the end users.

For admin UI, see the [AcS Help Desk Training for eSig.](#)

8.1.Interface Design Rules

The following design rules are applicable to the user interfaces for the eSig activities:

- The user and administrator interfaces comply with VA's branding specifications.
- The interface is easy to navigate with self-explanatory instructions/fields.
- The interface provides user friendly messages/information on error.
- The interface supports web browsers using Internet Explorer 7 (IE7), for Windows XP, IE9 for Windows7, and Mozilla Firefox3.6.23.
- The interface is Section 508 compliant (for non-administrator, end-user facing interfaces)
- The web interface provides necessary validation checks such as blanks for mandatory fields, special characters, and invalid email id format before form submission.

8.2.Inputs

The eSig activities are web pages, accessible via VA standard web-browsers. Navigation and data entry require no special devices beside mouse and keyboard, while meeting Section 508 compliance where appropriate.

Refer to section 8.4 for each of the web interface screen information regarding inputs to the system.

8.3.Outputs

In addition to web-based output and the ability to save web pages using native browser options, the following report media are generated by eSig:

- PDF
- WORD

8.4.Navigation Hierarchy

This section documents the navigation hierarchy for eSig activities that require the configuration of OOTB user interfaces.

8.4.1. Screen Shots

Please reference the [AcS Help Desk Training for eSig](#) to review all navigational screenshots.

9. Security and Privacy

This section will be updated based upon conversation between Rodney and Kevin

Data security is critical for VA to safeguard user information and ensure that data in motion as well as rest is secured properly. For the AcS 2.0, the following security measures and integrity controls are in place.

Data in Motion:

“Data in Motion” is secured using the combination of FIPS encryption and VA issued certificates. Internal communications between CA components are encrypted using the cryptographic libraries that meet FIPS requirement. CA IdentityMinder uses the Advanced Encryption Standard (AES) adapted by the US Government. CA IdentityMinder incorporates the RSA Crypto-J v3.5 and Crypt-C ME v2.0 cryptographic libraries, which have been validated as meeting the FIPS 140-2 Security Requirements for Cryptographic Modules. CA SiteMinder Policy Server uses certified FIPS140-2 (AES) compliant cryptographic libraries.

For communications outside of the AcS environment, certificates issued by VA Internal CA will be used for securing communications between the AcS and VA internal systems/applications and commercially trusted certificates will be used when the communication is exposed to external to VA clients and/or third parties.

Data at Rest:

The following table explains the “data at rest” points.

Table 28: Data Points and Security

Data Points	Data Type	Explanation
Oracle	Sensitive	<ul style="list-style-type: none">• Stores the IdentityMinder objects- sensitive user attributes.• Stores the audit log for SiteMinder and needs to be secured, but not encrypted, as there is no PII.• Stores the audit log for CA IDM and must be encrypted and secured for PII.• See vendor documentation for additional information regarding actual encryption algorithms used.
Directory	Sensitive	<ul style="list-style-type: none">• Stores encrypted SiteMinder policy data.• Stores SiteMinder/IdentityMinder user data. Only sensitive user attributes will be encrypted.• Provisioning server related objects and sensitive user attributes are encrypted.• See vendor documentation for additional information regarding actual encryption algorithms used.

Data Points	Data Type	Explanation
File Store	Non-Sensitive/ Sensitive	<ul style="list-style-type: none"> IM is stored in a JMS data in file system and contains transactional data. It does not contain any sensitive information. A FIPS encryption key file is stored in the file system. Access to the file should be restricted and enforced by setting the directory/file access permissions for specific groups and/or users.

The security controls for the data at rest are managed through the encryption of sensitive attributes at the directory level for the AcS 2.0. The FIPS 140-2 encryption is applied on the identified PII and sensitive attributes stored in the AcS 2.0 directory attributes. The following table provides the data types (refer to section A.1 below for data type groupings) and who can make updates accordingly.

9.1.Security

The requirements for Personally Identifiable Information (PII) are limited to data explicitly required in VA 6501 and NIST SP 800-63. However, the implementation adheres to the following integrity controls to ensure that acceptable security standards are met.

9.2.Privacy

The eSig service operates in a federated environment and requires that the user credentials that are being passed to it belong to an authenticated Level 2 or above user.

9.2.1. Confidentiality of Sensitive Information

The eSig service does not affect the user credential information stored within VA. No passwords are passed between user sessions. The reporting piece of eSig only records the events that occurred and does not affect any VA data.

9.2.2. Privacy of Personal Information

The eSig service does not store any sensitive PII of the user apart from the user id that is passed.

9.2.3. Process Integrity

The eSig service only allows for machine-to-machine sessions. The machine sessions are authenticated using the DataPower devices. The WebLogic servers only accept requests that are received through DataPower. The CoSign device is located within the internal VA network and is only accessible via the web service calls from the WebLogic servers.

9.2.4. System Availability

The eSig solution implementation is highly available and provides controls to minimize system failures, and access control to minimize man-made failures. The eSig service has hardware failover capability available within the CoSign product configuration. The DR environment hosts

a similarly configured setup as the primary Production site. For a detailed site-to-site replication setup, refer to section 6.2.8 for the eSig design information.

DRAFT

Attachment A – Approval Signatures

The signature below is an acknowledgement that the signatory understands the purpose and content of this document.

Signed: _____

_____ Integrated Project Team Chair and Business Sponsor Date

Signed: _____

_____ OIS Business Sponsor Date

Signed: _____

_____ IAM Program Manager Date

Signed: _____

_____ AcS Program Manager Date

Signed: _____

_____ Chief Architect Date

Signed: _____

_____ SDE Date

A. Additional Information

A.1. RTM

Refer obtain the RTM from the Rational Tool Concert Tool for a complete list of requirements documents that are applicable to the AcS 2.0.



Data Model
Elements - SDD emb

A.2. Packaging and Installation

The deployment package for Infrastructure will provide details for special considerations if any for each of the components. The CA SSO client is deployed as a package to the desktop by Enterprise System Engineering (ESE) team. Using the CA SSO client installation and configuration documentation and response files provided in the deployment package, the ESE package builds and automates the process of CA SSO client to users system.

A.3. Design Metrics

The design for IAM services is calculated based on requirements from PWS, BRD and CSP population estimates provided by VA.



VA CSP User
Population Estimates.

A.4. Acronym List and Glossary

The acronyms and terms used in this SDD are defined in the [Identity and Access Services Master Glossary](#).

A.5. Required Technical Documents

Refer to the CA vendor support/web site for detailed product documentation.

A.6. Attach Documents

Once the SDD is approved, submit the AERB Design Compliance Decision Certificate as an attachment to the completed and approved SDD.