

Submitted by  
**AbleVets  
DUNS: 078393180 CAGE: 6PE96**

15049 Conference Center Drive | Suite 500  
Chantilly, Virginia | 20151

**VistA Adaptive Maintenance (VAM)**

**SYSTEM BOUNDARY**

**MARCH 2018**

TABLE OF CONTENTS

[1. Purpose 1](#_Toc507761500)

[2. System Boundaries and Data Flow 2](#_Toc507761501)

# Purpose

The purpose of the VistA Adaptive Maintenance (VAM) project is to establish a secure, sustainable, high-performing, cloud-based service to implement provider workflow logic back-end processing and storage. The VAM service will replicate the Remote Procedure Call (RPC) functionality currently provided via VistA in a modern, well-documented platform (i.e., Node.js and NoSQL database). VAM will enable the incremental transition of clinical workflow logic out of VistA into VAM services, while maintaining full compatibility with current VistA clients such as CPRS. VAM will be hosted in production within the VA’s Enterprise Cloud (VAEC) using the Amazon Web Services (AWS) service provider.

# System Boundaries and Data Flow

VAM is comprised of 4 major architectural components:

1. **Veteran Integrated Care Services (VICS) Server** – Software component that comprises the individual Node.js-based services that comprise the overall suite of VAM services (called VICS). Service requests and associated data are sent from the client (e.g. CPRS, other) to the RPC Router and/or directly to VICS Server.

VICS Server exchanges data internally with its NoSQL JSON Datastore (see item #4 below). Data is sent back to client via the RPC Router (in the case of a CPRS client)

VICS Server Emulate limited set of VistA RPC (listed in Section 4). RPC Emulation provides

an opportunity to fully secure the RPC interface against illicit clients without affecting CPRS.

VICS introduce the ability to apply novel patient-centric access control policies. As the data

model of a VICS will clearly differentiate patient from other metadata, these services will

introduce the ability to apply novel, patient-centric access control, all without affecting CPRS.

This enhanced level of control will be covered in regression test suites.

1. **RPC Router** – implemented in Node.js, the Router received RPC requests from the client (e.g. CPRS, other) and forwards the RPC call to either the legacy VistA endpoint or to the cloud-based VICS Server for processing. The RPC Router is only used for client applications that leverage the legacy CPRS/VistA RPC calling format.

Traffic between the RPC router and VICS and between new clients and VICS over REST will be encrypted, and the effectiveness of that encryption will be tested. If Veteran Affairs add traffic encryption into and out of CPRS, VAM will add support to the router and test that encryption as well. Additionally, the RPC Router provides an auditing capability for all RPC traffic.

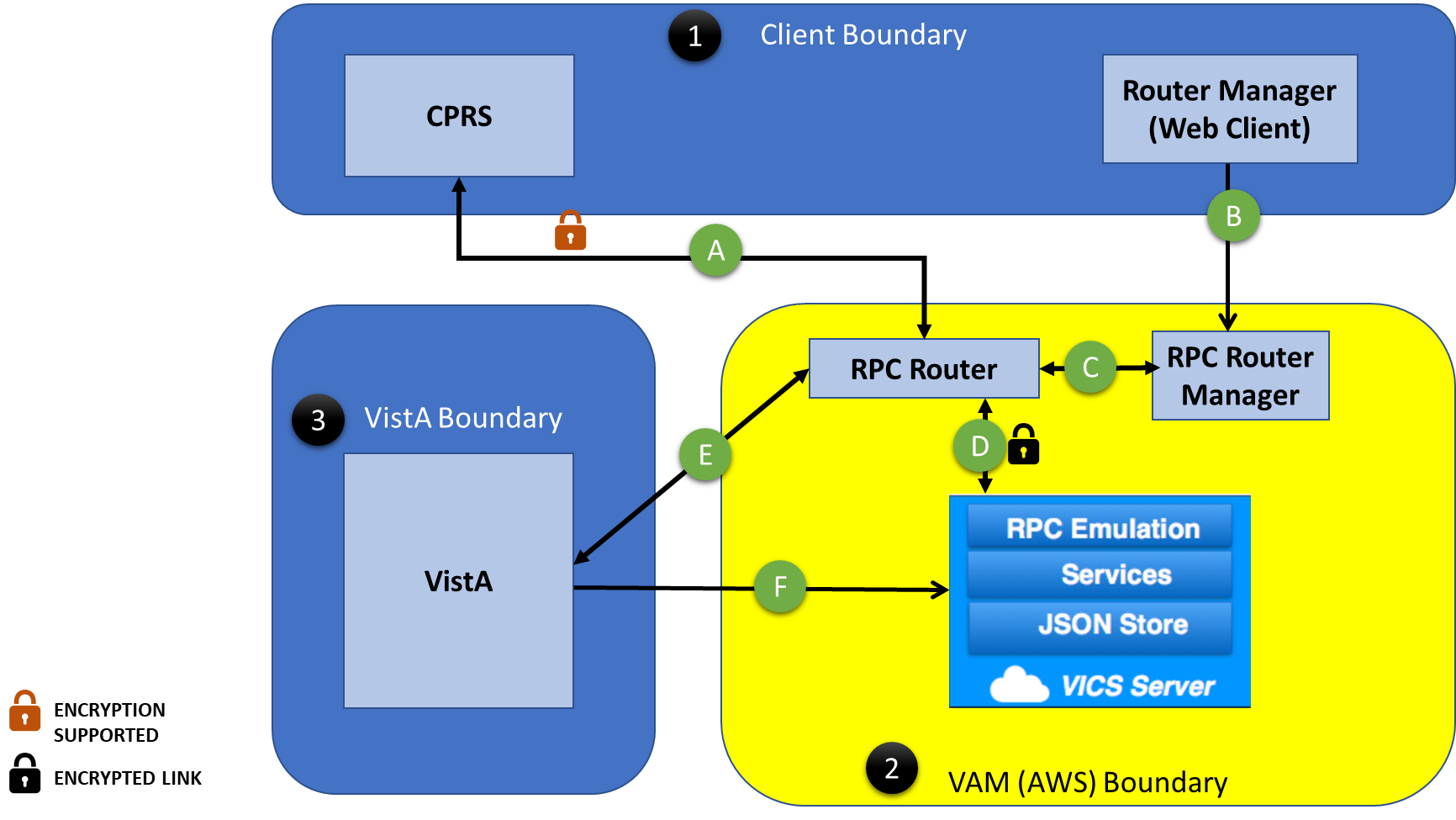
1. **RPC Router Manager** – Manages configuration and auditing of the RPC Router.
2. **NoSQL JSON Datastore** – Stores PII/PHI and non-PII/PHI electronic health record (EHR) data within FIPS 140-2 cryptographic modules for processing by the VICS services.

Note, all the above VAM components will be managed within a single security boundary, within VAEC. For illustrative purposes, Figure 1 (next page) depicts a typical usage scenario for VAM and the associated security boundaries. This Figure also represents the planned configuration for the IOC deployment. Figure 1 Data Flow link are described in detail on Table 1.

The three system and security boundaries are:

1. **Client Boundary:** The client application, CPRS in the case of the IOC, will be installed on a machine within end-user’s segment of the VA network. It will directly connect to the VAM Boundary through the VAECs Business Partner Extranet (BPE) ExpressRoute connection.
2. **VAM (AWS) Boundary:** VAM and its associated components (VICS Server, RPC Router, Router Manager, and Datastore) are all contained within a single security boundary within the VAEC using the AWS VA GSS. AWS VA General Support System (GSS) that is already documented within Risk Vision. All Security controls that are already documented in Risk Vision for AWA GSS cloud will be inherit within our System Security Plan (SSP). VAM will connect directly to the Client Boundary and the VistA Boundary through the BPE.
3. **VistA Boundary**: In the IOC/Figure 1 configuration, a VistA instance deployed within VA’s network will connect directly to the Client Boundary (to pass data to/from CPRS) as well to the VAM Boundary (to pass data to the Router and to support metadata sync) through the BPE.

#### **Figure 1: VAM Security Boundaries and Data Flow Diagram**



#### **Table 1: Data Flow**

|  |  |  |
| --- | --- | --- |
| **ID** | **Data Flow Link** | **Description** |
| A | CPRS to and from RPC Router | Data Flow between CPRS and RPC Router supports encryption. This link will carry RPC Calls, Meta Data and de-identified PII/PHI data. List of RPC and Data Elements are documented in separate document. |
| B | Router Manager Web Client to RPC Router Manger | This Link will carry REST calls to get Audit information. It will not contain any RPC Calls, Meta Data or de-identified PII/PHI data. |
| C | Router Manager to and from Router | This Link will carry REST calls to get Audit information. It will not contain any RPC Calls, Meta Data or de-identified PII/PHI data. |
| D | RPC Router to and from VICS Server | Data Flow between RPC Router and VICS Server is encrypted. This link will carry RPC Calls, Meta Data and de-identified PII/PHI data.  List of RPC and Data Elements are documented in separate document. |
| E | RPC Router to and from VistA | Data Flow between RPC Router and VistA is encrypted. This link will carry RPC Calls, Meta Data and de-identified PII/PHI data.  List of RPC and Data Elements are documented in separate document. |
| F | VistA to VICS Server | Data Flow from VistA to VICS server to sync Meta Data and de-identified PII/PHI data. |