Requirements Specification

Project MCCF_EDI_TAS (RM)

Prepared by Mann, Julie R. (Leidos)

November 5, 2018, 3:08:13 PM CST

Table of Contents

Introduction

The purpose of this document is to define the requirements.

TAS API Improvements and Security <RALLY ID US3816>

Artifact Content

User Story Name: TAS API Improvements and Security <RALLY ID US3816>

Sizing: 8

Story

As the... I need... So that...

TAS Business Owner Improvements made to the TAS API, including Security I can provide an application architecture for services and comply with VA SEC requirements

Conversation (if desired by developers)

• The TAS API used for non-VistA data access (non-FHIR) uses Docker for services scalability. Improvements will be made to the TAS API Docker implementation.

• By default, Azure Storage keys provide the equivalent of root access to all use access Azure Storage. Because of this, Azure Shared Access Signatures (“SAS”) are the preferred method of accessing Azure Storage. The recommended practice is to disconnect authorization (SAS) from authentication (keys).

• Storing secrets in or passing secrets directly into an application is not a recommended practice. Azure KeyVault provides a secure location for secrets and certificates while allowing selective access to them to authorized applications.

Signature Page

Frank C. Annecchini 1132102

Digitally signed by Frank C. Annecchini 1132102
Date: 2018.11.13 10:04:49 -06'00'

eBusiness Solutions

James S. Plastow 398558

Digitally signed by James S. Plastow 398558
Date: 2019.01.02 07:26:28 -07'00'

James Plastow, OIT PM