VistA Kernel Security

Department of Veterans Affairs

Office of Information and Technology (OIT)

March 2022

Version 1.0

Revision History

Date	Version	Description	Author
03/31/2022	1.0	Initial Version	VistA Office

Table of Contents

VistA Kernel Security

1. Introduction

Veterans Health Information Systems and Technology Architecture (VistA) Kernel is the intermediary layer between the host operating system and other VistA software applications, so that VistA software can coexist in a standard operating-system-independent computing environment. Kernel provides a standard and consistent user and developer interface between software applications and the underlying M implementation.

VistA Kernel Security is focused on the processes that will re-establish the Zero Trust security boundary for accessing VistA; as well as ensuring the VistA security boundary is upheld by all entities by utilizing established processes.

VistA Kernel Security has evolved over the years, and it has several components with various names and documented in different products. To better understand and describe the latest evolution in Security implementations in VistA, the Kernel Security Section contains a short description of the existing components, products, and their corresponding names and documents. The security aspects of this documentation will be mainly those in the category of User Identity Provisioning, User Authentication and User Authorization.

2. Processes

Enterprise VistA Environment Background Information: Enterprise VistA is comprised of virtual servers; RedHat Linux Operating System, InterSystems Cache, and InterSystems Cache and Inquiry Routing and Information System (IRIS) Database Monitoring Systems (DBMS), the VistA database application and over 100 M-based application modules. Each package is comprised of multiple software programs that includes administrative and clinical data. The VistA Kernel software provides identification and authentication, access control via menu management, and auditing of user actions. VA FileMan, the VistA database management software, in conjunction with the Kernel, provides data access control. Access to the system is controlled by set menus and security keys, which are determined prior to the initial issuance of access codes to new users or users who are changing positions within the organization. VistA is accessed by Secure Shell Layer emulators. To access VistA additional access is required via an Active Directory account, which requires two-factor authentication. All medical centers have production and pre-production test environments which are located within four VA data centers (Philadelphia, Austin, Sacramento, and Denver respectively.)

3. References

- Remote Procedure Call (RPC) Broker
  https://www.va.gov/vdl/application.asp?appid=23

- VistALink (XOBV)
  https://www.va.gov/vdl/application.asp?appid=163

- VistA Kernel
  https://www.va.gov/vdl/application.asp?appid=10

- M Programming Standards and Conventions SAC Document
  https://trm.oit.va.gov/RequestFiles/64102/M_Programming_SAC.docx

- IAM PIV Compliance
  https://dvagov.sharepoint.com/sites/OITEPMOIAM/playbooks/pages/piv%20compliance/piv%20compliance.aspx

4. Contact

For more information on VistA Kernel Security, please contact the VistA Process Governance Workgroup at VISTAProcessGovernanceWorkgroup@va.gov