VA Enterprise Design Patterns
Enterprise Architecture

Unified Communications Standards

OFFICE OF TECHNOLOGY STRATEGIES (TS)
OFFICE OF INFORMATION AND TECHNOLOGY (OI&T)

VERSION 1.0
DATE ISSUED: MAY 2017

APPROVAL COORDINATION

Gary E. Marshall 137891

Digitally signed by Gary E. Marshall 137891
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=gary.marshall@va.gov, cn=Gary E. Marshall 137891
Date: 2017.05.25 11:08:42 -04'00'

Gary Marshall
Director, Technology Strategies, ASD

Deeneen U Akeo 622220

Digitally signed by Deeneen U Akeo 622220
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=deeneen.akeo@va.gov, cn=Deeneen U Akeo 622220
Date: 2017.05.26 12:22:49 -04'00'

Deeneen Akeo
Acting Director, ASD

REVISION HISTORY

Version	Date	Approver	Notes
1.0	5/9/2017	Nicholas Bogden	Revised draft with new sections and added stakeholder feedback.

CONTENTS

Quick Jump

Select an icon to skip to a section.

Current Capabilities

Future Capabilities

Use Cases

One-VA Technical Reference Model

The Veteran-Focused Integration Process

Enterprise Design Pattern Scope

---

1 INTRODUCTION

The Department of Veterans Affairs (VA) offers a variety of electronic communications to interact with VA stakeholders. VA users can use electronic channels, such as Voice over Internet Protocol (VoIP), for efficient telephone communication; data networking, for information gathering and dissemination; video communication, to enhance communication to geographically distributed groups; and video content sharing, for broadening a communications network, narrowcasting, or providing a ubiquitous learning platform. VA users may select one specific form of communication (e.g., in-person, telephone call, text message, e-mail), or choose to adopt multiple forms of communication. All are necessary for VA to conduct its daily operations and fulfill its organizational mission. Currently, VA uses a mix of: (1) legacy forms of communications; (2) contemporary communications techniques; and (3) Unified Communications (UC).

UC capabilities are those that securely provide voice, video, and data service over a common network infrastructure. These include text messaging/chat functionality, video conferencing, and voice telephone calls. Further adoption of UC by VA can provide greater efficiency, cost savings, and new capabilities for some business functions.

The purpose of this document is to provide guidance on standards and architecture for the use of the current and future UC network infrastructure at VA. This document addresses areas of

interoperability, availability, quality, and security for VA UC. It is aligned with the FY2016-2018 Enterprise Roadmap modernization effort to converge and unify communications. The intent from this strategic guidance is to move all electronic communications to a single, IP-based network.[1]

1.1 Business Problem

VA uses various forms of voice, data, and video communications services, which provide necessary and valuable capabilities to support VA operations. Currently, however, there are several targeted areas identified for improvement in the use of communications devices and services. These include:

- Interoperability/Integration: VA facilities and programs do not have universal agreement on standardization, architecture, and policy to support deployment and integration of communications services. For example, VA facilities currently implement VoIP Session Initiation Protocol (SIP) systems, without an official VA policy that specifies standards.
- Availability: As a necessity to operations across VA facilities, communications services must be accessible to stakeholders. Yet communications services face challenges, including availability across the mix of legacy and newer technologies, limited support for mobile devices, and insufficient infrastructure to support high volume link sessions.
- Quality: Some VA implementations of communications have challenges with quality of service (QoS), reliability, and priority. VA does not have an enterprise policy on fully integrated voice QoS.
- Security: Some forms of VA communications (e.g., voicemail, fax, etc.) do not have contemporary security controls or standardized architecture in place.

1.2 Business Need

There is several technology and solution gaps that VA will need to address to resolve the business problems identified in section 1.1. These business/capability areas include:

- Interoperability/Integration: Greater interoperability and integration will require enterprise architecture planning (EAP), including the development of VA standards that

[1] See Department of Veterans Affairs FY2016-2018 Enterprise Roadmap, Office of Information and Technology, September 30, 2016, page 5.

support UC. A common, standardized technical architecture can alleviate silo effects within regions or districts.

- Availability: Achieving high levels of availability in communications services will require a planning process that defines the architecture for redundancy, modernization, and high-capacity usage.
- Improved Services: Greater adoption of common, commercial UC services will require a common architecture and appropriate hardware and software.
- Enhanced Security: Modern UC requires modern cryptography and security measures (e.g., secure document sharing) that are compliant with both Federal and VA policy.

These business needs will require VA to provide the technology infrastructure, funding, and other resources to support successful implementation. For example, communications services that include video technology, such as UC services, require a significant bandwidth allocation to achieve successful data transfer through a communications path. In addition, UC can require special hardware (e.g., handset phones or video teleconferencing equipment) and software. Project implementers will need to balance resources between current systems, current sustainment, and future implementation.

VA will also need to balance the enhancements to VA's communications infrastructure with guidance from Congress and the Government Accountability Office (GAO) to reduce the VA data center footprint. Reducing this footprint is also part of a VA strategy to move to cloud first and managed services. Resolutions to achieve this balance could include data center consolidation and the use of cloud services.

1.3 Business Case

This EDP aims to provide guidance to help facilitate UC at VA. It will enable VA to achieve the business benefits that are highlighted in Table 1. In general, increased standardization can lead to greater efficiencies, cost savings, interoperability, and security.

TABLE 1: BUSINESS BENEFITS

Business Benefits	Description
Economies of scale	• VA facilities that use common UC approaches can reduce acquisition costs when offices purchase similar equipment (as in group or collective buying). • Migration to modern UC approaches can reduce costs for hardware and maintenance (e.g., retiring fax machines, other older equipment, and other components of outdated or obsolete infrastructure). • VA facilities that use similar UC approaches can share best practices and knowledge, ultimately reducing support and maintenance costs. • VA facilities that adopt managed services or cloud services take advantage of the economies of scale offered by the providers, typically reducing costs.
Interoperability	• UC approaches using common interfaces promote greater interoperability. • Multiple VA applications can use improved information integration. For example, multiple operators could share call center patient data and transfer the data when operators transfer a call. • Some forms of UC offer common user interfaces across devices.
Improved availability	Modern UC technology offers techniques, such as packet-switched networking, to improve availability.
Improved services	VA's use of standard approaches can provide new services that aid VA operations (e.g., telehealth, text chat for support and call centers, real-time monitoring/oversight of VA call centers, or other operations).[2]
Security	Standard, documented approaches allow implementers to use common security approaches, improving VA's overall security posture.

[2] UC monitoring is often separate from UC services. Different, separate vendor products may provide the monitoring services and the communication services.

This EDP will help modernize the VA communications infrastructure, provide guidance on achieving new capabilities, and provide approaches that can lead to efficiencies and cost savings. VA project implementers will often need to integrate UC with existing VA technology investments. In some cases, the UC approaches presented in this EDP will be necessary at certain VA sites, as the traditional legacy services are phased out by carriers (e.g., VoIP SIP may replace voice Time Division Multiplexing (TDM) Primary Rate Interface (PRI) capabilities). Where this occurs, migration to UC is significant for ensuring business continuity.

1.4 Approach

The approach recommended by this EDP addresses the business problems discussed in section 1.1. In particular, this document will address the following:

- Interoperability/Integration: The EDP will provide recommended standards and approaches to address UC. Documentation of common approaches and technical design patterns will aid future VA efforts and support improved interoperability. This includes integration of VoIP and voice-as-a-service (VaaS), as well as how to integrate these when using an external UC provider.
- Availability: A description of architectural components will address a general approach for ensuring availability. Where feasible for various applications, this EDP will recommend network characteristics.
- Quality: The EDP will detail considerations for any performance gaps with UC solutions and provide corresponding recommendations/mitigations. In particular, this document will discuss network controls, on-net communications, and user interfaces. It will also reference wiring standards.
- Security: Content on risk mitigation strategies for UC approaches will explain how to address UC security.

Section 2 will describe current communications capabilities. Section 3 provides explanations of techniques and technologies to modernize VA's approaches to communications. Section 4 will detail VA UC use cases.

2 CURRENT CAPABILITIES AND LIMITATIONS

VA uses several forms of communications technology, such as:

- Software-based solutions that rely on Microsoft Lync for chat/instant messaging functionality, desktop sharing, and voice/video capability

- Telecommunications infrastructure for hard phones, soft phones, and wireless phones
- Print centers for document sharing and fax service
- A Veteran Relationship Management (VRM) program that uses a Customer Relationship Management (CRM) Unified Desktop
- Large scale video teleconferencing systems, including hardware and software-based endpoints, gatekeepers, gateways, content recorders, and multipoint conferencing systems

Many of these technologies are UC elements that VA provides over a data packet-switched network. This section describes these capabilities in detail and identifies areas for process improvement.

2.1 Interoperability/Integration

Across the organization, VA is procuring and implementing many types of communications technologies that are not standardized and may not be fully interoperable or integrated.

Integrating communications systems can provide cost savings from avoiding vendor lock-in.[3] Regardless of the number of different products used, VA improves its overall communications through integrated and interoperable systems.

In particular, the following situations occur across VA:

- Currently, sites may use multiple types of systems for redundancy, a practice which supports availability in the event of an outage, but may be an impediment to interoperability. An example of this type of redundancy is Microsoft Lync and Avaya audio bridging systems supporting the Veterans Affairs National Telecommunications System (VANTS).
- The flexibility to introduce new technology may be inconsistent with the enterprise architecture. This may be the case when a new technology is first introduced.
- VA does not have a lab facility to conduct full scale interoperability testing. Accordingly, there is not a central service that can help guarantee interoperability.
- Some areas of VA do not have consistent infrastructure to support greater use of UC. Examples include insufficient backup power, insufficient power, non-standard cabling, and insufficient cooling and ventilation.

[3] An analysis of expenses can more accurately determine the most cost effective approach. A variety of equipment may add expense and technical challenge for support, sustainment, and maintenance.

- Organizations are reluctant to dispose of existing equipment (e.g., Polycom, Tandberg), so implementers need to determine how to integrate and support this equipment. This should be part of ongoing lifecycle replacement planning.
- Organizations often use different vendor products, either by design, or by accumulation over the course of several years of operation.
- In SIP implementations, some vendor standard implementations may not be 100% compliant with basic international standards or may not interoperate fully with other vendor implementations. If the SIP protocol is used, systems need a way to translate between multiple vendor variants.

Organizational planning, funding, and support are essential for the success of any efforts towards VA-wide interoperability and integration in the UC community. This includes support from all levels in the organization.

2.2 Availability

VA sites face multiple challenges in maintaining overall availability of communications services. The causes include the following:

- VA sites may not have a variety of options in last mile connectivity. Accordingly, a single incident may disconnect a medical center. If a network provider's connections drop, sites that use cloud services for communications will have service interruptions.
- Currently, some telecommunications carriers are discontinuing Time Division Multiplexing (TDM) voice PRI circuits or making these harder to acquire. Instead, these providers are only offering VoIP SIP.
- Some forms of VA UC lack full features on all device types. For example, mobile device software (e.g., Microsoft Lync, Skype) may not be as capable as the UC software clients for other platforms. In modern organizations, users will typically have one or two different endpoint devices.
- The availability of forms of UC depends on the technology, implementation, and network or carrier that supports it. Some implementations of UC may not have adequate redundancy and resiliency.
- Some VA sites have difficulty supporting high volume link sessions due to bandwidth and other constraints.
- Ideally, UC services support all platforms for both internal and external VA staff (e.g., Windows, iOS, Android) to include robust mobile, remote access to services and staff.
- Remote VA locations may be challenged with implementing service expansions.

2.3 Quality

Some VA sites may face technical and organizational challenges in supporting high quality UC when implementing QoS, reliability, and priority. Some characteristics of quality may be more difficult to support when using UC forms of communications. For example, VoIP may experience network delay, jitter, signal attenuation, and compression. Individual VA sites may not be currently enforcing the implementation of the same VA baseline LAN, QoS, and other network parameters. Tools and systems should be put in place to adequately monitor and measure the overall quality of UC systems.

2.4 Security

Some VA sites have difficulty meeting all of the existing security requirements for implementing communications systems. Legacy forms of communications (e.g., fax machines) may also have limited security controls in place. Greater coordination and standardization may help improve the overall communications security posture at VA.

VA sites that implement new forms of communications, such as messaging/chat lines for a call center, may face difficulties in securing these systems. Security is especially critical as VA communications systems may be used to transmit Personally Identifiable Information (PII), Protected Health Information (PHI), and sensitive business operation information. These communications are subject to the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.

An organization's UC network can be the weak link for security. This area is often targeted by adversaries, due to known vulnerabilities. There are numerous types of exploits for UC systems. In integrated systems, if an adversary captures credentials, the adversary can open all related services. For example, compromised Microsoft credentials from one service will open up One Drive, Skype, and other Microsoft accounts. In many government and commercial organizations, communications toll fraud is rampant and a source of monetary loss. For example, a toll fraud adversary may gain control of a UC phone dialing system and call a phone number that charges high tolls. This will increase VA phone charges dramatically. In these scenarios, the adversary earns money from the incident because the adversary has ownership or interest in the toll number.

3 FUTURE CAPABILITIES

The use of communications technology at VA will evolve. This section addresses how VA can improve its UC systems through greater standardization, architecting for availability, and ensuring quality, security, and alignment to: (1) the One-VA Technical Reference Model (TRM) and (2) the project management tool known as the Veteran-focused Integration Process (VIP). Section 3.7 provides a summary of this future state.

Table 2 describes the various business benefits that future UC capabilities can provide.

TABLE 2: BUSINESS BENEFITS OFFERED BY FUTURE CAPABILITIES

Business Benefits	Description
Interoperability and Integration	• Use of interoperable equipment can lead to cost savings. For example, group buys for similar equipment can lower purchase and support costs, due to less variation in equipment purchased. • Where possible, future capabilities will align to specified standards and specifications. This will promote common interfaces that allow for interoperability, regardless of which technology providers are used.
Highly Available Services	Use of UC must also properly support VA operations in high volume use cases by providing highly available and robust services.
Enhanced UC Services	Greater use of common UC approaches will help plan for future expansion of services, allowing for the introduction of new UC services, where it has not previously been used (e.g., introduction of new chat features, mobile services, expansion via cloud or managed services).
Assuring UC Security	Modern UC services may be able to replace some legacy services. Such new UC services often enable the use of modern cryptography and security features.

The following figure is a diagram of the general UC vision. It shows how VA can transform separate legacy systems into UC systems that use a common network. This illustration provides a high level view of how UC could exist at VA. It does not, however, specify a time frame for implementation. Many pieces of telecommunications equipment, including enterprise level networking equipment and end user devices, such as phones, have a life span of 10 or more years. It is not expected that equipment needs to undergo an early retirement and disposal.

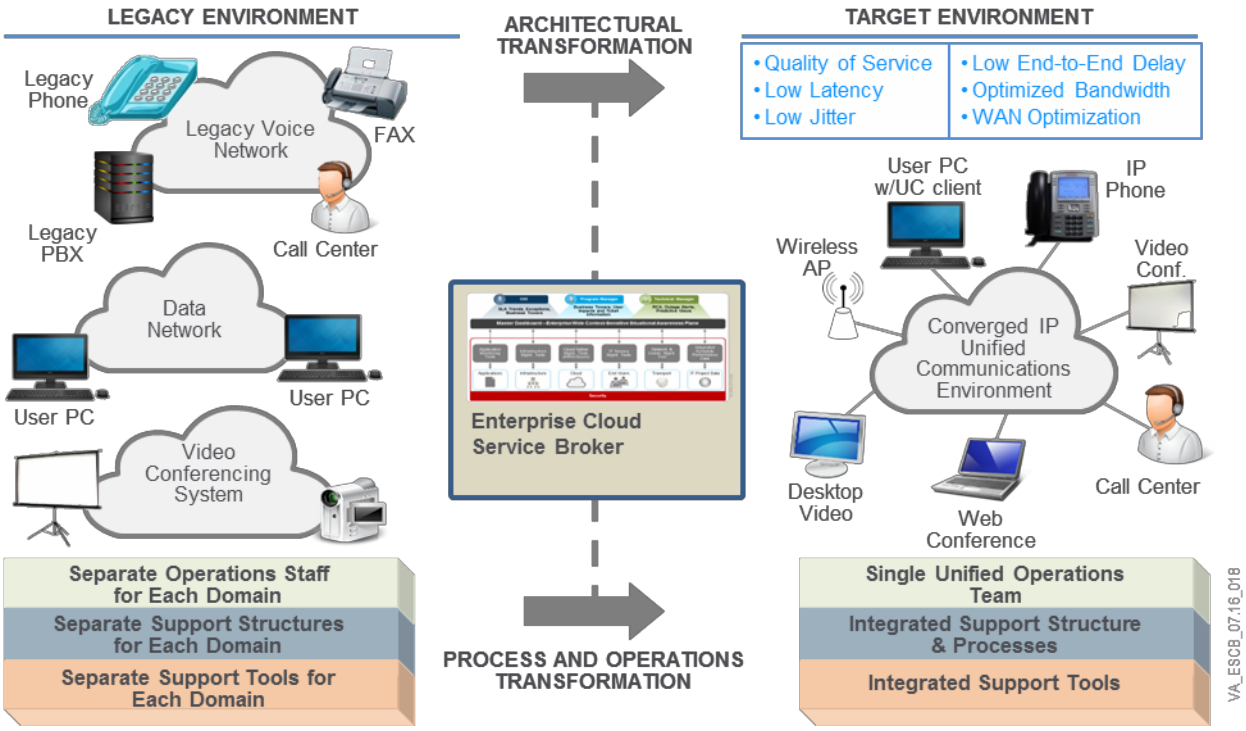

FIGURE 1: US TRANSFORMATION DIAGRAM

VA can provide these capabilities either on premise or via cloud resources. Implementers can also develop these systems in a virtualized fashion. In these cases, the system should still meet all required VA policies and adhere to the patterns presented in the subsequent subsections of this section of the document.

When VA organizations lease, obtain managed services, or plan outsourcing of UC functions, these organizations must coordinate with relevant VA technical/engineering staff to ensure that these contracts are legal and technically feasible. This will ensure alignment of these efforts with current VA virtualization and cloud efforts. Additionally, VA staff should consider methods for contracting outsourced services that allow for adequate oversight of the services. VA should contract such services on a finite time line so that VA can periodically assess and potentially reassign such services.

Deploying a new UC system or modifying existing UC capabilities will not singularly fix all communications problems. Rather, VA will also need to align the deployment of UC technology with appropriate business processes and staffing requirements.

3.1 UC Interoperability and Integration

This section provides an overview of the common standards that implementers should use when considering new and expanded UC within VA to promote interoperability and integration. UC needs to work across numerous use cases: mobile/remote, web-based, home office, work office, small group space, large space, and boardroom. This section will not prescribe certain products or vendors, but will provide information to help ensure that interfaces and protocols are consistent to ensure interoperability. Readers can find additional details on alignment with the One-VA TRM in Section 3.5.

Typically, organizations have existing communications equipment and need to consider prior technology investments and infrastructure when building a UC system. Usually, the starting point is some existing infrastructure and equipment that is critical to the organization. This accumulation of different vendor's equipment with different life spans may occur over time or may be part of a plan. Telecommunications equipment (e.g., phones) often has a shelf life of 10 years or more. Integrating equipment of various ages results in additional challenges for effective UC interoperability planning.

To address these issues and challenges, the following sections outline how VA can improve interoperability through effective oversight, organizational planning, standards, Session Border Controllers (SBC), interoperability validation testing, session management, centralized management, managed services, consolidation, and line of business integration.

3.1.1 Oversight

Greater integration of communications systems will enable better management and oversight of VA operations. For example, call center statistics on call wait times, queue times, and other parameters can give management a real time impression of the effectiveness of the center. This will enable more targeted training and real-time correction of problems. VA systems can use such monitoring to ensure security in real time.

3.1.2 Organizational Planning

Effective organizational planning involves a thorough understanding of the business requirements, organizational structure, technical and regulatory requirements, existing systems,

and other potential constraints. Additional planning elements in the UC community can include ensuring compatibility with a unified national dial plan that includes telephony, Video, IM/chat, presence, and SIP URI dialing.[4] Depending on the scope and goals of each project, VA organizations may also need to consider additional technologies and features in implementing each system.

For example, there is a current effort to implement a VA national UC system core that will support the integration of voice, video, and IM communications systems by creating a standardized point where existing UC systems can federate with each other in a vendor agnostic environment. This will reduce operational silos (e.g., phone, mobile client, video system, IM) and further implement the VA strategic vision.

3.1.3 Session Initiation Protocol

To support interoperability, VA organizations will use UC equipment, systems, and services that support fully open industry standards and protocols to enable cross-vendor operation. The requirements for these operations include the ability to conduct and end sessions, as well as negotiate between the various codecs used in a UC session.

Products that support vendor proprietary codecs must also be able to support open standards to allow interoperability with other vendor products. Ensuring that the interfaces in the system allow interoperability will help to avoid vendor lock-in. This can yield economic benefits over time by supporting future purchases. It will also help to ensure that products can be fully utilized until replaced or discontinued.

One of the key standards for the UC environment is SIP. This is the primary protocol for UC and VoIP. UC systems often contain components that support various other standards.

In future UC efforts, VA should use SIP as the standard and divest from older TDM trunks, except for use as backup. Where VA uses SIP, SIP normalization is important to ensure interoperability across different vendor implementations of SIP. Equipment, such as SBC, can provide SIP normalization functionality.

VA can use SIP in a number of use cases, including:

[4] The Enterprise Voice project created the National Multiprotocol Signaling Cloud that ties different phone systems together. It supports Uniform Resource Identifier (URI) dialing and a video network.

- Door phone
- Audio alert
- Callbox
- Multimedia intercom
- SIP cameras for video surveillance
- Network clocks
- Paging systems
- Signaling protocol for Web Real-Time Communication (WebRTC)
- Supporting video conferencing systems
- Connecting to cloud communications services
- Computer Telephony Integration (CTI) (connecting to servers and software)
- Connections with Internet of Things (IoT) devices
- Connections with VoIP gateways
- Trunking between IP Private Branch Exchanges (PBX)

The SIP session management layer can provide a common point for codec, protocol, and dial plan normalization. For example, a multi-protocol session manager or a call control manager can translate from SIP to H.323 natively, without a separate gateway. Such a manager could also communicate and translate numerous other protocols, such as Skinny Client Control Protocol (SCCP) and Media Gateway Control Protocol (MGCP).

Network architecture can use centralized SIP trunking between locations, but also support different protocols at the edge. This can help with migrations and is often cost effective. A centralized architecture also allows for disaster recovery and redundancy options.

Because VoIP is based on Transmission Control Protocol (TCP)/Internet Protocol (IP), it can transit a dedicated circuit, or be comingled with data traffic on multiuse circuits (e.g., Skype on internet connection). Voice service provider architectures fall into two main camps: those who isolate voice traffic (e.g., by keeping it on the Public Switched Telephone Network (PSTN) only), air gapped from other networks (e.g., internet), and those who leverage their data network infrastructure for both voice and data.

Based on the latest version of the Department of Homeland Security (DHS) Trusted Internet Connections (TIC) program, VoIP traffic is not in the scope of the TIC initiative. In a future version of TIC, DHS may expand the scope of TIC to cover VoIP. Keeping VoIP as a separate connection, such as a PSTN connection that is not comingled with data, will allow VoIP traffic to ingress outside the TIC gateways.

In lieu of implementing TIC connectivity for SIP, VA projects may choose to consider the following connection options. Implementation of any of these options as a standard will require design and implementation of a standard architecture in VA.

In the first external SIP connectivity option, shown in Figure 2, the SIP provider circuit terminates on a VA managed SBC or equivalent device. The connection handoff to the VA network is either PRI (TDM) or IP.

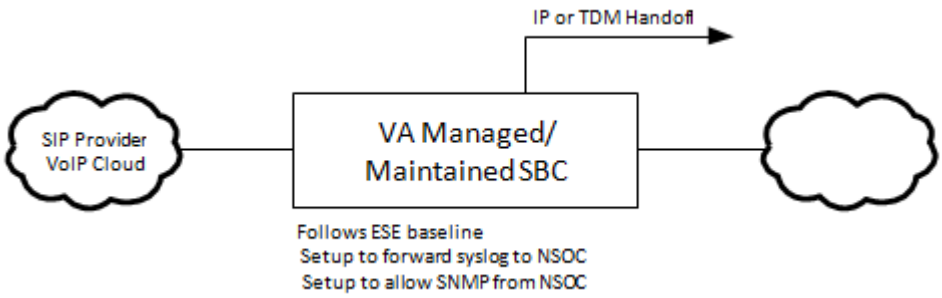

FIGURE 2: OPTION 1, SIP PROVIDER CIRCUIT TERMINATES ON A VA MANAGED SBC

In the second external SIP trunk connectivity option, the SIP provider circuit terminates on an SBC or equivalent device that is carrier provided and managed. The connection handoff to the VA network uses IP traffic.

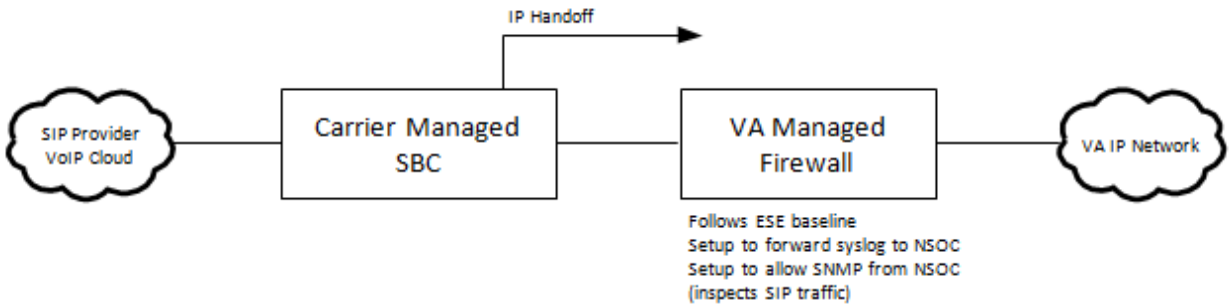

FIGURE 3: OPTION 2, SIP PROVIDER CIRCUIT TERMINATES ON CARRIER-PROVIDED AND -MANAGED SBC

In the third option, depicted by Figure 4, the system uses a carrier managed SBC or equivalent system. In this option, the inside handoff to the VA network is a PRI TDM link. Since this handoff uses PRI TDM, there is no IP traffic to inspect.

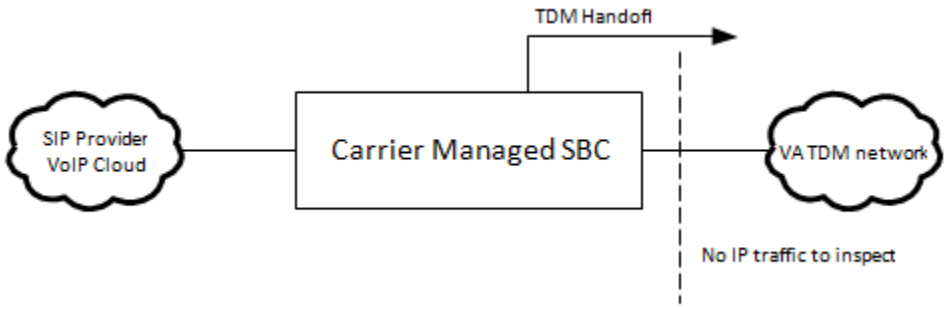

FIGURE 4: OPTION 3, SIP PROVIDER CIRCUIT TERMINATES ON CARRIER-PROVIDED AND -MANAGED SBC

3.1.4 Session Border Controllers

A SBC is a device deployed in VoIP networks to control the signaling and media streams for setting up, conducting, and ending telephone calls or other interactive media communications.

Where possible, VA should acquire and deploy standardized SBCs that support multiple protocols and codecs. SBC products will pass any content an end point needs to communicate with local and remote parties. It will do this in real time and not slow down the communication. VA will not need to mandate a strict requirement to endpoints on what protocols to use. For example, Skype for Business may use a codec like SILK, whereas Cisco can only use G.722. A SBC will transcode between these to facilitate the communications.

The use of SBCs at VA can support termination of VoIP services at facilities if done using a set of VA-approved standards that cover security and device management.

3.1.5 Interoperability Testing

A standardized lab environment is essential for ensuring the effective and secure deployment of new UC systems. Such a lab can determine issues before deploying UC changes to the production system. Troubleshooting new and existing UC systems and applications in a production environment can be difficult. It is often impractical and adds additional risk to the VA network. Most UC implementations are multi-vendor, and vendors often hold each other responsible for problems that may arise.

To ensure proper interoperability and integration of UC products, VA will need to establish and manage an interoperability lab, or gain access to a facility or organization that can test for

interoperability.[5] This lab would verify that different UC components fully interoperate within the VA enterprise. VA can use a lab at any time to test new products or configurations. VA should ensure interoperability testing prior to network infrastructure configuration changes (e.g., use of interoperability lab). To establish a VA UC lab, VA will need to staff the lab with knowledgeable UC engineers to manage it and run tests.

Lab testing can also identify performance and operability issues. For example, unexpected traffic spikes can lead to problems. An interoperability lab can help by providing stress tests and numerous types of network tests.

One of the requirements of any VA UC lab is to have a standardized approach and plan for testing. There can be a wide variety of UC implementations. Testers should assume each system is unique. There can be differences in SIP protocol headers, differences in error codes, dual tone multi frequency (DTMF) signaling requirements, and even blockage of 911 calls. In addition, fax works differently with nearly every SIP trunk provider. Testing by VA implementers should verify the functionality and software releases used in the systems.

3.1.6 Session Management

A session management layer provides a natural point for protocol, codec, and dial plan normalization and implementation. This is available under different product names (e.g., session director, platform, session manager edition, session manager) from different vendors. It provides a more standardized interface for federation/integration across the enterprise and outside of the enterprise (e.g., PSTN access, mobile/remote access, conferencing services). It would address and support User Datagram Protocol (UDP) and Transport Layer Security (TLS) termination.

3.1.7 Centralized Management

Where possible, UC systems should also implement centralized management of UC functions and systems to ensure consistent configuration and accuracy. Where policies and updates are centralized, systems also provide labor savings. This use of centralized services saves time because there is not a need to connect to each UC component and individually configure it.

[5] A defense example of this is the Department of Defense Joint Interoperability Test Command (JITC).

3.1.8 Managed Services / Cloud Services

Another approach that VA can employ to aid interoperability is the use of managed services. In part, this requires that managed services support interfaces for interoperability. In general, these approaches align with the VA cloud first initiatives and efforts to reduce on-premise server footprints.

Regardless of the scenario, managing UC services either as a managed service or in the cloud can be done by leveraging a management infrastructure that allows organizations to handle UC functionality just like any other application in the cloud. When a VA organization selects a cloud service, ideally this service will also support UC integration or a hybrid UC approach.[6]

The benefits of running UC in the cloud are similar to those of other cloud-based applications. These include business continuity/failover among geographically distinct data centers; the ability to scale services up and down as needed; and cost efficiencies that are inherent with cloud computing services. In addition, the cloud makes mobility better and simpler. Among the biggest benefits of mobility is that it provides "anywhere, anytime" access to corporate data and collaboration tools.

However, transitioning 100% of services to managed services or the cloud can take many years. For example, Netflix took seven years to implement cloud services.

3.1.9 Consolidation

VA should consider consolidation of platforms to reduce the number of UC platforms that need support and maintenance. This further reduces the challenges and complexity in maintaining older platforms that are not maturing toward convergence within the enterprise or using cloud services. It helps to consolidate voice platforms that are not evolving toward cloud convergence. UC technology updates should be incorporated into standard lifecycle replacement programs.

3.1.10 Line of Business Integration

Where supported by requirements and a cost analysis, unified communications solutions should integrate with VA's business applications. For example, contact centers often support multiple methods of communication (e.g., phone, video, text chat) and have an integrated system to

[6] Additional details on cloud computing services can be found in the Cloud Computing Architecture, Cloud Security, Enterprise Cloud Services Broker, and Platform-as-a-Service EDPs.

respond to Veterans. For such line of business applications, the desktop, mobile, and web clients should integrate with the UC. Ideally, this could be supported for traditional server, cloud, and hybrid deployments.

3.2 Architecting for High Availability

This section addresses how to ensure availability in UC solutions. The approach taken for assuring availability should consider the desired application and its requirements to set a standard level of uptime. VA implementers should also assess each piece of vendor equipment to assure it can meet the required availability for the desired application.

To support availability, VA implementers should can consider the basic tenants of redundancy, failover, call control, and networking, as outlined in the following subsections.

3.2.1 Redundancy

VA should consider implementation of backup and failsafe services in case of emergencies or network outages.[7] VA organizations should conduct a study of requirements, the need for availability, technical challenges, and cost analysis to determine the type of redundancy and backup needed on a site-by-site basis. Any redundancy measures need to consider security and operational procedures. Options for increasing redundancy include:

- Implement managed service or cloud-based backup solutions, such as UC as a Service.[8]
- Use a diversity of external carriers to provide multiple independent network connection options.
- Design and implement a UC solution with more than one of each essential function (e.g., implement an SBC and a secondary/backup SBC).
- Additional back-up redundancy is possible, as long as there is an IP connection. If a mobile device loses a cloud connection, the system could still use the mobile device's connection to get to a gateway.

[7] For more information, readers may consider consulting the Business Impact Analysis EDP, which covers how to assess risk and impact related to the Primary Mission Essential Functions. Readers may also consult the Disaster Recovery Planning EDP that covers the process of immediate recovery of critical IT systems to normal operations in the event of a disaster or extended critical disruption at a VA facility. Emergency Management Teams leverage information from relevant system Business Impact Analysis (BIA) and Information System Contingency Plan (ISCP) documents along with guidance and policies outlined in NIST 800-34 and VA Handbook 6500.8 to develop a Disaster Recovery Plan (DRP) for their respective facilities.

[8] Readers may also consider consulting the Disaster Recovery Planning EDP and a forthcoming Disaster Recovery as a Service EDP. These describe methods of preparing for and determining methods of adding redundancy and resiliency.

- For voice service, a VA project could implement a backup using TDM or analog phone service. Figure 5 depicts connectivity with analog phones. Analog phone service is standardized. It tends to be a low cost phone solution, and offers numerous features (e.g., caller ID, call waiting, call forward). Analog will still use the legacy wiring, the same way TDM/digital phones would. Analog systems that do not support IP voice can be adapted to IP transport through an appropriate gateway. Formulating a standard practice to converge TDM based systems into the network will save on expenditure of funds on new equipment and provide the redundancy of the PBX backbone that is required.

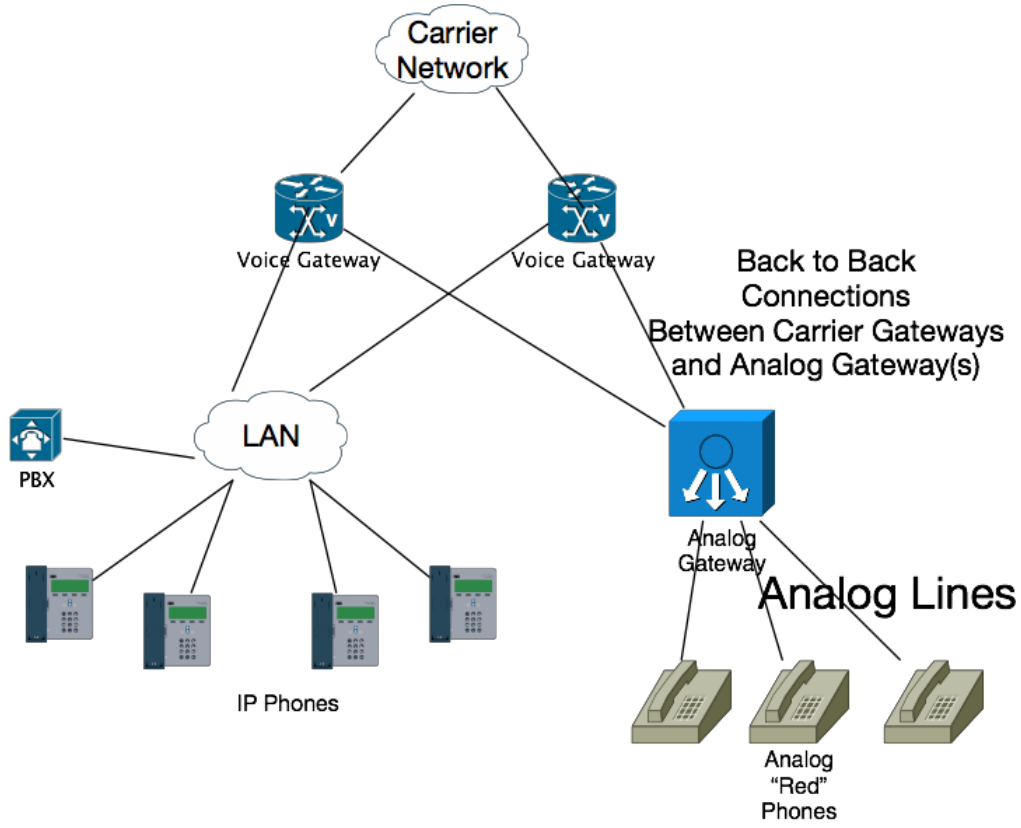

FIGURE 5: VOICE SERVICE NETWORK DIAGRAM WITH ANALOG BACKUP

3.2.1 Failover / Call Overflow

It is important to engineer for local and system-wide failover, or engineer a call overflow between two functions in your network. Failover is a communication feature where a standby computing system takes over when the main system fails. Call overflow is the implementation of

failover for voice connections. For example, an organization could implement a centralized call center to have call overflow between a Northeast region and a Southeast region.

Overflow treatments are available on TDM, IP PBX, automatic call distributors (ACD), and SBCs. These features can be invoked externally, using alternate trunk groups with different point codes; internally, using an overflow hunt list; and via virtual call center applications.

3.2.2 Call Control

VA can implement a call control plan that includes the use of call control over IP and using the carrier network as a backup. Such a system can re-route calls to another gateway, adding or removing digits as necessary, without user intervention or knowledge.

3.2.3 Networking

VA can enhance availability through techniques for regional availability and geographic availability. Regional high availability provides multiple services within the same state or region. These services all share the workload within that region. Geographic high availability uses multiple, independent regional sites; high traffic loads and failures can trigger sharing of the workloads among these different geographic sites.

A diversified SIP trunking approach can aid availability and continuity of operations to achieve load balancing between systems. VA should engineer this to allow for redundant components within regions. Additionally, carrier diversity can also aid availability. In the event that one carrier's service is down or facing difficulties, the other carrier services may still be functional.

VA should design UC services for a multi-vendor environment. Multi-vendor environments have better availability. This recognizes that existing equipment across VA is from many vendors and these will continue operation. This also helps to increase availability and resiliency from the use of many different products. System administrators should ensure there are two vendors to deliver SBC functionality for a system.

3.3 Providing Unified Communications (UC) Quality

This section addresses how to maintain appropriate quality within the UC environment. It discusses aspects of network controls, on-net communications, user interfaces, and wiring standards.

UC should implement network traffic controls to aid the real time nature of communications. VA implementers must prioritize and isolate network traffic to avoid garbling, packet loss, and

static. This includes priority marking, priority queuing, and establishing appropriate interfaces. Additionally, VA should use UC management systems to ensure that overall QoS, latency, and jitter are within established Service Level Agreements (SLAs) and standards.

Real time communications, such as voice packets, cannot tolerate packet loss. VA should implement standard VA QoS and have the tools to verify that this is functioning.

On-net communications offer efficiency and can aid UC quality provided the internal network offers the proper level of service. Standard VoIP features include dialing on-net, toll bypass, and tail end hop off to help keep traffic on the internal network. Tail end hop off is where most call routing is on-net, and just the tail end travels over another network.

Where feasible, to aid users of UC features, implementers should procure or design consistent user interfaces across different end user devices (e.g., hard phones, mobile smart phones, tablets, and computers). This will improve user experiences and aid in user training and understanding of solutions.

Lastly, VA facilities and implementers should follow VA standards and guidance provided by Information Technology Operations and Services (ITOPS) Solution Delivery. These standards and guidance cover wiring standards and electrical power standards (e.g., UPS) for both in-house and network facilities. Ensuring that the physical layers of the network comply with these standards is critical to ensuring the overall functionality and ultimately the overall quality of the UC applications that use this transport.

3.4 Unified Communications (UC) Security

This section addresses the security of UC services including risks and mitigations for these risks. Across VA, facilities are deploying a greater number and variety of endpoints (e.g., embedding communications into applications, smart phones, devices, computers, hard phones). New forms of UC can enable retirement of legacy services that were not as secure (e.g., retire fax machines and replace with secure document storage services). This section defines and discusses data in transit encryption requirements, protocols, and end-user device characteristics (e.g., unique certificates per device). It also covers securing data at rest, including applying encryption for voice mails. Separate from this document, there is general computer and networking security information available from other VA EDPs and outside guidance documents.[9]

[9] Additionally, cybersecurity documents are also available from the National Institutes of Standards and Technology (NIST). Other materials on topics including UC, securing a server, and network security are available from the Defense

3.4.1 Authentication

All VA UC systems should implement user authentication, a critical piece of effective cybersecurity. Multi-Factor Authentication should be implemented wherever possible. Implementers can base this on factors such as "something you have," "something you know," and "something you are." Authentication with SIP/TLS can use three factors (i.e., user name, password, and certificate). VA has documented additional details on user authentication in the User Identity Authentication EDP. For more information, see the User Identity Authentication EDP.[10]

3.4.2 Confidentiality

VA security requirements stipulate that there must be end-to-end encryption of data and signaling using NIST Federal Information Processing Standard (FIPS) 140-2 [11] validated cryptographic modules on call control and endpoints. Migration of services to SIP can ease the implementation and use of FIPS encryption. Where technically possible, these SIP trunks should have FIPS 140-2 validated encryption.[12] Systems using legacy PSTN and TDM trunks typically do not have encryption. Readers should consult the Data Storage EDP for additional information on confidentiality of data.

VA mandates the use of secure protocols wherever possible. These include protocols and services such as TLS, Secure Real Time Protocol (SRTP), Internet Protocol Security (IPSec), Hypertext Transfer Protocol Secure (HTTPS), Institute for Electrical and Electronic Engineers (IEEE) 802.1x for port based network access control, mobile device management (MDM) virtual private network (VPN), and public key infrastructure (PKI) active directory (AD) single sign on (SSO).

3.4.3 Network Considerations

UC equipment can also perform real time monitoring of network and communications security. For example, an SBC can offer real time monitoring of UC traffic, which can include inspection of traffic beyond that performed by typical firewalls.

Where VA uses SIP, SBCs can enhance the UC system's security posture. SBCs can offer support for secure protocols such as SIP-TLS, secure RTP support, and IPsec tunneling support. SBCs also

---

Information Systems Agency (DISA). Interested individuals should look up the Security Technical Implementation Guides (STIG) and the Security Requirements Guides (SRG).

[10] This document is available at the following link: https://www.techstrategies.oit.va.gov/enterprise_dp.asp

[11] FIPS 140-2 is the US Government computer security standard used to approve cryptographic modules.

[12] A list of validated FIPS 140-1 and 140-2 cryptographic modules can be found at this site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

provide a firewall rule set while mapping Open Systems Interconnection (OSI) layer 5 to OSI layer 7 application addresses. SBCs offer intrusion detection and prevention as well as support for Denial of Service (DoS) attack identification and prevention. VA can use SBCs to implement VPN separation for shared resources.

VA could replace services, such as fax, by secure cloud fax services. Such an implementation may also yield cost savings on support and a reduction in the requirement for analog ports.

Additionally, when designing a network to support UC systems, consider network functions that can mask the underlying network topology. This feature can aid the overall system's security posture by obscurity.

All VA UC solutions must conform to a variety of technical requirements including FedRAMP, TIC, and VA 6500 handbook security requirements. VoIP (to include external SIP trunking) is currently out of scope for TIC version 2.1. However, in future versions of TIC, the DHS may bring VoIP into scope. VA programs should adhere to any new updates to the TIC program. These security guidelines apply for any VA UC service moved to the cloud, any VA facilities migrating to SIP trunks from TDM PRI, any UC services that VA newly acquires, or any outsourced VA UC service.

Devices that connect to the VA network will have to adhere to the DHS Continuous Diagnostics and Mitigation (CDM) program.[13] Such devices include Medical Device Isolation Architecture (MDIA) devices, mobile devices, and devices that connect via remote VPN. Based on this program, endpoint devices will need to support vulnerability and security testing. UC systems should also support proactive monitoring.

3.4.4 Logging, Auditing, and Reporting

For security, all UC systems should have a mechanism for centralized logging and auditing of UC transactions. For voice applications, the UC system should also support retention of Call Detail Records (CDR), based on Federal and VA policy including VA 6500.[14] In accordance with VA Records Control Schedule (RCS) policy, we have to keep CDR records for a minimum of three years

[13] For more information, please see https://www.dhs.gov/cdm. Additionally, CDM is referenced in other EDP documents including: Vulnerability Management, Enterprise Auditing, and Configuration Management.
[14] Readers may also want to consult the Enterprise Auditing EDP v1.0 or any newer update if available, which discusses logging.

and one day. In call center applications, the UC system should have reporting capabilities to assist with management. For additional information, refer to the Enterprise Auditing EDP.[15]

3.5 Alignment to the One-VA Technical Reference Model (TRM)

All projects will leverage approved tools and technologies located in the One-VA TRM[16] to comply with the architectural guidance provided in this document. The following table lists the approved tools for this Enterprise Design Pattern (EDP).

TABLE 3: LIST OF APPROVED TOOLS AND STANDARDS FOR UNIFIED COMMUNICATIONS

Technology Category	Example Technologies	Example Standards
Networking	• TCP/IP • Authentication • Session Initiation Protocol • Virtual Local Area Networks (VLAN)	IEEE 802.1X, IEEE 802.1Q, IETF RFC 3261
Voice	• VoIP Session Initiation Protocol (SIP), Primary Rate Interface (PRI)	IETF RFC 3261, ITU-T I.431
Vocoder	• Pulse code modulation • Algebraic Code Excited Linear Prediction (ACELP) • Wideband audio codec	ITU-T G.711, G.729a, G.722
Video-conferencing	• Visual telephone systems and terminal equipment	H.320, H.323, H.225, H.460

3.6 Alignment to Veteran-Centric Integration Process (VIP)

This EDP informs technical standards for the underlying infrastructure of capabilities delivered under VIP. VIP is a Lean-Agile project framework. VIP services the interest of Veterans through efficiently streamlining activities that occur within the enterprise. The VIP framework unifies and streamlines IT delivery oversight. VIP delivers IT products more efficiently, securely, and predictably. VIP is the follow-on framework from the Project Management Accountability System (PMAS) for the development and management of IT projects. VIP will propel the Department with even more rigor toward Veteran-focused delivery of IT capabilities.

[15] This document is available at the following link: https://www.techstrategies.oit.va.gov/enterprise_dp.asp.
[16] http://trm.oit.va.gov/

More information on VIP can be found at https://vaww.oit.va.gov/veteran-focused-integration-process-vip-guide/.

3.7 Summary

3.7.1 Considerations for Requirements

Projects that implement UC solutions should incorporate requirements based on this EDP into the project requirement documents and IBM Rational tools. The following table highlights key areas of content that may help projects to develop requirements for future UC systems at VA.

TABLE 4: CONSIDERATIONS TO INFORM REQUIREMENTS

Section #	Requirements Considerations
3.1 UC Interoperability and Integration	VA organizations will leverage approved networks and infrastructure. VA projects will coordinate with ITOPS prior to deploying solutions on the VA network.
3.1.2 Organizational Planning	VA implementers will integrate UC system dial plans to ensure connectivity between all necessary VA facilities and external party facilities.
3.1.3 SIP	VA projects will implement systems capable of fully open industry standards to promote interoperability. UC systems will migrate to SIP as the standard and divest from TDM trunks, except for resiliency. VA implementers will retain legacy TDM trunks and other necessary legacy technologies for emergencies and network outages. VA UC implementers will include SIP normalization functionality within their designs to ensure interoperability between different SIP implementations. UC systems will include gateway functionality to translate between H.323 and SIP and between TDM and SIP.
3.1.4 SBC	VA projects will implement SBCs or equivalent functions to ensure interoperability in systems that communicate media streams.

Section #	Requirements Considerations
3.1.5 Interoperability Testing	VA implementers will conduct interoperability testing for all UC functionality. VA implementers will ensure interoperability testing prior to network infrastructure configuration changes.
3.1.6 Session Management	UC systems will include a common session management layer for protocol, codec, and dial plan normalization.
3.2 High Availability	VA organizations will conduct technical and cost analysis to evaluate options for UC redundancy.
3.3 Providing UC Quality	UC systems will ensure communication quality by appropriately marking real-time and non-real-time communications packets, appropriately queuing UC packets, and implementing appropriate interfaces.
3.4.1 Authentication	Systems will use multi-factor authentication in UC systems.
3.4.2 Confidentiality	UC Systems will implement end-to-end FIPS 140-2 encryption on UC systems.
3.4.3 Network Considerations	UC systems will perform real time monitoring of UC communications traffic. UC systems will implement network topology hiding for UC networked components. UC systems will implement centralized logging and auditing that is based on VA RCS policy and VA 6500.

3.7.2 Recommended Standards

The following table outlines recommended future state standards for adoption within VA UC.

TABLE 5: RECOMMENDED UC STANDARDS

Standard Name	Standard Reference
SIP	IETF RFC 2543, IETF RFC 3261, and subsequent updates/clarifications

4 USE CASES

4.1 Use Case 1: Phasing Out Voice Primary Rate Interface TDM Connectivity and replacing it with Voice Over IP Session (VOIP) Initiation Protocol (SIP)

4.1.1 Purpose

In this use case scenario, a VA medical center is seeking to migrate voice services from legacy voice PRI to more modern VoIP SIP trunking services. Many VA facilities are finding that telephone providers are phasing out TDM handoffs using Voice PRIs. In some locations, only VoIP SIP is available, whereas in others, only PRI is available. To address a facility moving to SIP, this use case will describe best practices for VoIP SIP and high volume link sessions.

4.1.2 Assumptions

This use case assumes that appropriate network infrastructure is installed with appropriate controls and configuration (e.g., a separate VLAN is established for VoIP), or can be updated. It also assumes that SIP-based hardware and handsets are available. In general, starting with voice may aid later transitioning to other UC services.

4.1.3 Use Case Description

In this use case, a local network manager seeks to migrate a system from voice PRI to VoIP SIP. This migration can yield several benefits. New VoIP SIP functionality can more easily provide status information, caller ID, and additional services. SIP services are generally more scalable. VoIP solutions may lower overall costs and reduce or minimize costs for add-on services (e.g., conference lines, fax lines, call recording). VoIP also allows flexibility for staff who travel frequently or who work remotely. A SIP migration can also work with analog phones and support fax, alarm lines, and related equipment.

The VA facility should start with a SIP readiness assessment to identify what to transform. The implementers can follow this with a standard design process that creates architecture, evaluates vendors, and completes a SIP design. In architecting this system, it is important to consider the need for availability and redundancy and consider having a failover between two functions in the network. An organization could have a centralized call center for the northeast region or the southeast region to have failover between them. Another consideration for implementations that require high availability is a multi-carrier architecture to reduce the possibility of problems occurring on all carrier networks simultaneously.

Designs need to consider what service providers can provide. In some cases, only certain buildings or sides of a street are within a coverage area. The implementer needs to consider the variants of SIP that may be necessary for different aspects of the coverage area. A designer needs to take each element and consider its location, dial plan requirements, and physical terminal components. It is important to figure out where to connect SIP trunks.

The implementation of this system needs to consider whether a cloud based VoIP solution or on-premise VoIP solution best meets the system requirements. Different factors may play into whether it is best to implement this in-house or use an external cloud service provider. HIPAA and federal regulations will limit cloud provider choices.

Forklifting all services at once to a managed cloud solution can include risk; it can be expensive and limit the time that is necessary to evaluate the solution before the implementer finalizes it. Accordingly, the network administrator should move to implement SIP at the organization's own pace to work out any issues with quality such as jitter or low Mean Opinion Scores (MOS). Later, when the SIP implementation is stable, the administrators should cut the legacy voice service.

Upon completion of a design, the facility should conduct a test and pilot the technology. Organizational planning or integration needs to occur in order to include developing dial plan details for SIP transformation. It is important to verify that the procured equipment will function with the telecommunications carrier and other VA systems. Different implementations of VoIP SIP may not support interoperability with other vendor's implementations. System testing is also a key component to ensuring operability and interoperability.

Once a successful pilot of the technology is complete, VA implementers should plan a phased roll out of services more widely across their targeted facilities. A transformational phase can reduce overall risk. VA implementers should not rush into a SIP transformation. It can be helpful to address an office user group before servicing an entire building. During a migration, implementers can check to see if a phone or device is connected. If not, they can connect a phone back to a PRI trunk, and then to the PBX.

SIP transformation governance should establish guidance on how to manage and upgrade components, and how to change service providers. For SIP service management, it is important to recognize ongoing management and monitoring services.

4.2 Use Case 2: Implementation of New UC Services Including Video on Demand

4.2.1 Purpose

In this use case scenario, a VA medical center is seeking to implement new UC video services to improve operational performance and access to care. The use case will discuss practices for doing this effectively, efficiently, and securely.

4.2.2 Assumptions

This use case requires a video connection and appropriate hardware and software. This capability is applicable across VA; however, certain applications may have higher utility (e.g., Veterans Crisis Line call center).

4.2.3 Use Case Description

This use case describes video conferencing in VA environments. Video conferencing is useful in many communication scenarios as a close approximation to real-life, in-person discussions, remote care, and counseling. It generally offers elimination of travel expenses and time, as compared to in-person meetings, and improved quality of communication, such as greater retention of information and improved access to care.

On the other hand, video content is technically demanding. It requires high bandwidth to communicate imagery, audio, and control messaging. It also requires low latency, low jitter, and high reliability.

In some circumstances, flexibility in migrating between a text chat, voice call, or video conferencing session is invaluable. VA responders could use this capability in cases where a Veteran is in crisis, such as in a suicidal state. Visual contact with a Veteran during a time of crisis may be highly desirable. It may also be beneficial to have a video capability on personally owned cellular phones.

WebRTC is one tool that can enable secure, real-time communication with call centers. A Veteran making contact with a crisis phone line on a personally owned smartphone could use WebRTC to enter a video conferencing session. This can be encrypted and use digital authentication. WebRTC allows a web browser to become audio/video endpoint using call control and HTML 5. It can integrate with WebRTC endpoints and Lync end points with proprietary codecs. VA implementers can use UC Application Program Interfaces (APIs) to integrate this into web sites, so that a Veteran could access this feature from a VA site.

VA implementers should implement a standard web API that can launch the WebRTC session for the Veteran. This would allow access from a smartphone. This use of WebRTC can involve an SBC to translate between systems using older standards and newer systems using SIP.

Before beginning transformational services, implementers must perform transformation planning and identify the risk and its impact on scheduling. This can include transformation to LAN and LAN components. It will also include definition of QoS requirements and designs. The effort will need dedicated resources to execute the long-term strategy.

For security, VA implementers should approach different components separately. System implementers need to conduct an analysis of Federal and VA policy, guidance, and requirements to appropriately configure and secure the UC equipment.

VA has many locations and users. When deploying this solution, it can be valuable to phase in functionality over time to appropriately test and integrate each facility and user community.

The use of UC, in this case, can enable other features, such as a standardized view and a virtualized wallboard that brings critical call center information. This provides real-time updates that could enable leadership to view the health status of VA's call center environment. With an ability to display anomalies, it could improve responsiveness and productivity.

APPENDIX A. SCOPE

This EDP provides an enterprise-level view of the "As-Is" and "To- Be" mobile capabilities that are relevant to Veteran-facing mobile applications and the standard processes in use. The document refers to, rather than duplicates, lower-level solution guidance associated with these capabilities.

- This EDP focuses on:
- Guidance for UC architecture using appropriate standards
- Providing common guidance for all forms of UC
- Security and risk mitigations
- A set of use cases that will allow VA to implement VoIP in a standardized way throughout the enterprise

The EDP document is generally applicable across all VA Lines of Business (LOB) and describes:

- "As-Is" VA UC capabilities
- Future state VA UC infrastructure and capabilities
- Processes to be used by implementers and users of UC
- Enterprise-level UC constraints and terminology

This EDP document does *not* address detailed technical solution guidance for implementing specific UC hardware of applications. It will only provide the constraints to drive VA UC projects towards development of solutions that effectively meet the specific goals of their initiatives.

Topics that are out of scope for this EDP include:

- Use of TIC access providers when the UC service type is not supported
- Vendor specific products or implementation details

Document Development and Maintenance

This EDP was developed collaboratively with internal VA stakeholders, including participation from VA's Office of Information and Technology (OI&T), Enterprise Program Management Office (EPMO), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Information Technology Operations and Services (ITOPS). In addition, the development effort included engagements with industry experts to review, provide input, and comment on the

proposed pattern. This document contains a revision history and revision approval logs to track all changes. Updates will be coordinated with the Government lead for this document,

which will also facilitate stakeholder coordination and subsequent re-approval, depending on the significance of the change.

APPENDIX B. DEFINITIONS

This appendix provides definitions for terms used in this document, particularly those related to databases, database management, and data integration.

Key Term	Definition
Access	Interaction with a computer system for instance VistA. Such interaction includes data retrieval, editing (create, update, delete) and may result from a variety of technical mechanisms including traditional user log on, consuming applications exercising middleware based connectivity, SOA service requests, et cetera.
Analog Phone	A phone that uses analog electrical signals to place phone calls, which are usually sent over the Public Switched Telephone Network (PSTN); in general, one line can handle one call at a time, but analog phone service supports a number of additional features. Analog phone service is sometimes referred to as Plain Old Telephone Service.
Auditing	The inspection or examination of an activity based on available information. In the case of computer systems, this is based on review of the events generated by the system or application.
Primary Rate Interface	A telecommunications interface standard used to provide multiple voice and or data connections; PRI is part of the Integrated Services for Digital Network (ISDN) standards.
Public Switched Telephone Network	The worldwide circuit switched telephone network operated by a collection of local, national, and regional operators.
Session Border Controller	A network function that controls media streams, establishment and discontinuation of connections, call setup, and media session controls; SBCs often provide security and monitoring functionality, transcoding and translation between different vendor media and protocols, quality of service functions, and other features.
Session Initiation Protocol	A protocol used to establish a communications session between two or more parties; SIP can set up and control voice calls as well as other forms of communications (e.g., file transfer, presence information, text chat).
Time Division Multiplexing	A communications technique that allows multiple signals to communicate over the same channel by assigning different periodic time slots to each signal.

Key Term	Definition
Unified Communications	Communications services that integrate voice, video, and data over the same infrastructure; UC integrates both real-time (e.g., instant messaging (chat), presence information, telephony, video conferencing, data sharing (including web connected electronic whiteboards), and non-real-time (e.g., integrated voicemail, email, Short Message Service (SMS) and fax) forms of communication. UC is not a single product, but a set of products that provides a consistent unified user interface and user experience across multiple devices (both fixed and mobile) and media types (voice/audio, video, text). Through the use of basic UC capabilities or through the use of communication-enabled business process (CEBP), UC can optimize business processes and enhance human communications by reducing latency, managing flows, and eliminating device and media dependencies.
Unified Communications Monitoring	A service that monitors UC in an enterprise; a separate vendor may provide the Unified Communications Monitoring service.

APPENDIX C. ACRONYMS

The following table provides a list of acronyms that are applicable to and used within this document.

Acronym	Description
ACD	Automatic Call Distributor
ACELP	Algebraic Code Excited Linear Prediction
AD	Active Directory
API	Application Program Interface
ASD	Architecture, Strategy, and Design
CRM	Customer Relationship Management
CEBP	Communication Enabled Business Process
CTI	Computer Telephony Integration
DHS	Department of Homeland Security
DoS	Denial of Service
DTMF	Dual Tone Multi Frequency
EPMO	Enterprise Program Management Office
FIPS	Federal Information Processing Standard
GAO	Government Accountability Office
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
ITOPS	Information Technology Operations and Services
ITU	International Telecommunications Union
LOB	Lines of Business
JITC	Joint Interoperability Test Command
MDM	Mobile Device Management
MGCP	Media Gateway Control Protocol
MOS	Mean Opinion Score
NIST	National Institute of Standards and Technology

Acronym	Description
OIS	Office of Information Security
OI&T	Office of Information and Technology
PBX	Private Branch Exchange
PII	Personally Identifiable Information
PHI	Protected Health Information
PKI	Public Key Infrastructure
PMAS	Project Management Accountability System
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RCS	Records Control Schedule
RFC	Request for Comment
SBC	Session Border Controller
SCCP	Skinny Client Control Protocol
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
SOA	Service Oriented Architecture
SRTP	Secure Real Time Protocol
SSO	Single Sign On
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TIC	Trusted Internet Connection
TLS	Transport Layer Security
TRM	Technical Reference Model
TS	Technology Strategies
UC	Unified Communications
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
VANTS	Veterans Affairs National Telecommunications System
VLAN	Virtual Local Area Network
VistA	Veterans Health Information Systems and Technology Architecture
VoIP	Voice Over Internet Protocol

Acronym	Description
VPN	Virtual Private Network
VRM	Veterans Relationship Management

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

This EDP is aligned to the following VA OI&T references and standards applicable to all new applications being developed in the VA, and are aligned to the VA Enterprise Technical Architecture (ETA):

#	Issuing Agency	Applicable Reference/ Standard	Purpose
1	VA	VA Directive 6551	Details a mandatory policy for establishing and utilizing Enterprise Design Patterns by all Department of Veterans Affairs (VA) projects developing information technology (IT) systems, in accordance with VA's Office of Information and Technology (OI&T) integrated development and release management process, the Veteran-focused Integration Process (VIP).
2	VA OIS	VA 6500 Handbook, http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=56	Establishes an information security program in VA, which applies to all applications that leverage ESS.
3	DoD CIO	Department of Defense Unified Capabilities Reference Architecture	Provides common language and reference for DoD implementation of UC technology; it also lists common UC standards and specifications.
4	DISA	DoD Unified Capabilities Approved Product List (APL), http://disa.mil/network- services/ucco	Provides a list of products that have successfully completed DoD interoperability and security certification.
5	DoD CIO	Unified Capabilities Requirements 2013 (UCR 2013) Change 1, http://www.disa.mil/ucco- files/UCR-2013-Change1-Main.pdf	Provides DoD's Unified Capabilities requirements.

#	Issuing Agency	Applicable Reference/ Standard	Purpose
6	DISA	AS-SIP 2013 Change 1, http://www.disa.mil/uc co-files/AS- SIP-2013-Change1.pdf	Provides DoD's Assured Services Session Initiation Protocol.
7	DISA	UC XMPP 2013 Change 1, http://www.disa.mil/uc co-files/UC- XMPP-2013-Change1.pdf	Provides DoD's Unified Capabilities Requirements.
8	DISA	Telecommunication Security Technical Implementation Guides (STIG), http://iase.disa.mil/stigs /net_perim eter/telecommunication s/Pages/in dex.aspx	Provides DoD technical implementation guidance for securing systems.
9	VA	VA Directive 6513, "Secure External Connections," http://www.va.gov/vap ubs/viewPu blication.asp?Pub_ID=5 02&FType=2	Provides policy and responsibilities for secure external connections to VA networks.
10	VA	VA Enterprise Roadmap http://vaww.ea.oit.va.g ov/wp-content/uploads/2016/ 09/2016092 8_FY-2016-2018-Enterprise-Roadmap.pdf	Provides high level strategy related to VA enterprise IT including UC convergence for infrastructure modernization.

#	Issuing Agency	Applicable Reference/ Standard	Purpose
11	VA	VA Directive 6517, "Risk Management Framework for Cloud Computing Services," http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=8	Provides VA's cloud first policy.
12	VA	Office of Construction & Facilities Management Telecommunications and Special Telecommunications System Design Manual,	Provides requirements for telecommunication engineering and design.
13	VA	VA Electrical Design Manual, December 2015, https://www.cfm.va.gov/til/dManual/dmElec.pdf	Provides electrical design guidance for safe, reliable, and energy efficient installation.
14	VA	Physical Security Design Manual, January 2015, https://www.cfm.va.gov/til/PhysicalSecurity/dmPhySecLS.pdf	Provides physical security standards for VA facilities and projects.

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.