

Prepared for:

Federal Communications Commission

**CMS Alliance to Modernize Healthcare
Federally Funded Research and Development Center**

Contract No. 75FMC18D0047

Task Order No. 273FCC19F0144

Video Access Technology Reference Platform (VATRP) Release Documentation

Version 1.1

July 31, 2019

The views, opinions, and/or findings contained in this report are those of The MITRE Corporation and should not be construed as official government position, policy, or decision unless so designated by other documentation.

Approved for Public Release; Distribution Unlimited. Public Release Case Number 19-2187

© 2019, The MITRE Corporation. All rights reserved.

Record of Changes

Version	Date	Author / Owner	Description of Change
1.0	January 2, 2019	Health FFRDC	Additional information corresponding to v1.0 release, including an updated test plan. Version 1.0 for publication by Sponsor.
1.1	July 31, 2019	Health FFRDC	Additional information corresponding to v1.1 release, including an updated test plan and record of known and resolved issues. Version 1.1 for publication by Sponsor.

Executive Summary

The Federal Communications Commission (FCC) Telecommunications Relay Service (TRS) Center of Expertise (COE) Project promotes the Commission’s goal to foster innovations that advance functionally equivalent telecommunication services for members of the d/Deaf or hard of hearing community. The project helps ensure that the TRS employs improved technology for persons who are d/Deaf, hard of hearing, DeafBlind, and/or have speech disabilities. The MITRE Corporation (MITRE) is using d/Deaf as an umbrella term to describe individuals who are deaf in the audiological sense, as well as those who identify as culturally Deaf. While not all people identify with solely one or the other, MITRE is using “big-D” Deaf to describe individuals who identify primarily as members of an ethno-linguistic culture (or linguistic and cultural minority) and “little-d” deaf to describe individuals who primarily identify as deaf in the medical or audiological sense.

At the FCC’s request, MITRE independently assesses voice telephone services, video access services, and Internet Protocol (IP) Captioned Telephone Service (CTS); improvements to TRS efficiency; solutions for direct communication between persons with who are d/Deaf, hard of hearing, DeafBlind, or who have speech disabilities using telecommunication technologies; and the effectiveness, efficiency, and consumer response to delivering TRS.

The Centers for Medicare & Medicaid Services (CMS) Alliance to Modernize Healthcare federally funded research and development center (FFRDC) is the first FFRDC dedicated to strengthening the nation’s healthcare system. This FFRDC is referred to as the Health FFRDC. MITRE, an objective not-for-profit organization, operates the Health FFRDC in partnership with CMS and all HHS agencies to implement innovative ideas to solve our nation’s toughest health problems.

At the FCC’s request, the Health FFRDC developed a Video Access Technology Reference Platform (VATRP) in support of the FCC’s Accessible Communications for Everyone (ACE) program. This platform was developed in accordance with the Relay User Equipment (RUE) Specification to serve as a standards-based test platform for interoperability. Table ES-1 presents the new VATRP features for this release.

Table ES-1. New VATRP Features

Version	Release Date	New Feature or Capability
0.1	December 3, 2018	<ul style="list-style-type: none"> • One stage dial-around • Session Initiation Protocol (SIP) over Transport Layer Security (TLS) encryption • Changed application logo from “ACE” to “VATRP” • Registration patches for Proxy server and configurable port
1.0	January 2, 2019	<ul style="list-style-type: none"> • Adaptive Rate Control • Patch for Datagram Transport Layer Security (DTLS) support and for calls placed using an unsupported encryption • Additional test cases in the test plan
1.1	July 31, 2019	<ul style="list-style-type: none"> • Network Address Translation (NAT) Traversal • Video quality features (PLI, PFU, FIR) • Patches for DTLS, xCard, anonymous calls, config file loading

Table of Contents

1. Introduction	1
1.1 Background	1
1.2 Purpose and Scope	1
2. Release Notes	2
2.1 Release History	2
2.2 Known Issues	3
2.3 Resolved Issues	3
3. Installation Guide.....	5
3.1 Quick Installation	5
3.2 Installation from Source Code.....	6
3.2.1 Installing Microsoft Visual Studio.....	6
3.2.2 Building the VATRP	6
4. User Guide	8
4.1 Registration	8
4.2 Placing a Call	10
4.2.1 Placing an Encrypted Call.....	10
4.3 Features	12
4.3.1 Real-Time Text.....	12
4.3.2 Contacts	13
4.3.3 Message Waiting Indicator	14
5. VATRP Test Plan.....	15
5.1 Registration	18
5.1.1 Registration Test.....	18
5.1.2 SIP over TLS Encryption.....	19
5.2 Geolocation and Contact Information	19
5.3 Current Call Features	20
5.3.1 Call Quality.....	20
5.3.2 Media Encryption	21
5.3.3 Audio Mute and Video Privacy	21
5.3.4 Dual-Tone Multi-Frequency	22
5.3.5 Real-Time Text.....	22
5.3.6 Pause Call	23
5.4 Additional Call Features.....	23
5.4.1 Multiple Registered RUEs.....	23
5.4.2 Anonymous Calls.....	24
5.5 Message Waiting Indicator.....	25
5.6 Contact List Management	25
5.6.1 xCard.....	25

5.6.2 CardDAV	26
5.7 One-Stage Dial-Around.....	26
5.8 Emergency Calls	27
Acronyms.....	28
Notice	30

List of Figures

Figure 1. Screenshot of VATRP Setup Wizard	5
Figure 2. Screenshot of VATRP Login Screen.....	8
Figure 3. Screenshot of VATRP Main Window.....	9
Figure 4. Screenshot of Call View	10
Figure 5: Enabling encryption using DTLS.....	11
Figure 6: Generate and export a new “linphone-dtls-default-identity.pem”.....	12
Figure 7. Screenshot of Call View with Chat	13
Figure 8. VATRP Traceability Matrix for Tests Involving Multiple Calls	16
Figure 9. VATRP Traceability Matrix for Tests Conducted Once Per Provider.....	17

List of Tables

Table 1. VATRP Version History.....	2
Table 2. VATRP Known Issues.....	3
Table 3. VATRP Resolved Issues.....	3
Table 4. Registration Statuses.....	9
Table 5. Point-to-Point Call Procedure	18
Table 6. Registration Test.....	18
Table 7. SIP over TLS Encryption Test.....	19
Table 8. Geolocation and Contact Information Test.....	19
Table 9. Subjective Video Quality Test Criteria.....	20

Table 10. Subjective Audio Quality Test Criteria	20
Table 11. Media Encryption Test.....	21
Table 12. Audio Mute and Video Privacy Test	21
Table 13. DTMF Test	22
Table 14. RTT Test.....	22
Table 15. Pause Call Test.....	23
Table 16. Multiple Registered RUEs Test	24
Table 17. Anonymous Call Test	24
Table 18. Message Waiting Indicator Test	25
Table 19. xCard Test.....	25
Table 20. One-Stage Dial-Around	26

1. Introduction

The Federal Communications Commission (FCC) Telecommunications Relay Service (TRS) Center of Expertise (COE) Project promotes the Commission's goal to foster innovations that advance functionally equivalent telecommunication services for members of the d/Deaf or hard of hearing community. The project helps ensure that the TRS employs improved technology for persons who are d/Deaf, hard of hearing, DeafBlind, and/or have speech disabilities. The MITRE Corporation (MITRE) is using d/Deaf as an umbrella term to describe individuals who are deaf in the audiological sense, as well as those who identify as culturally Deaf. While not all people identify with solely one or the other, MITRE is using "big-D" Deaf to describe individuals who identify primarily as members of an ethno-linguistic culture (or linguistic and cultural minority) and "little-d" deaf to describe individuals who primarily identify as deaf in the medical or audiological sense.

At the FCC's request, MITRE independently assesses voice telephone services, video access services, and Internet Protocol (IP) Captioned Telephone Service (CTS); improvements to TRS efficiency; solutions for direct communication between persons with who are d/Deaf, hard of hearing, DeafBlind, or who have speech disabilities using telecommunication technologies; and the effectiveness, efficiency, and consumer response to current and future approaches to delivering TRS.

The Centers for Medicare & Medicaid Services (CMS) Alliance to Modernize Healthcare federally funded research and development center (FFRDC) is the first FFRDC dedicated to strengthening the nation's healthcare system. This FFRDC is referred to as the Health FFRDC. MITRE, an objective not-for-profit organization, operates the Health FFRDC in partnership with CMS and all HHS agencies to implement innovative ideas to solve our nation's toughest health problems.

1.1 Background

As part of the Accessible Communications for Everyone (ACE) program, the Health FFRDC independently assesses voice telephone services, video access services, and Internet Protocol (IP)-based captioning technology; improvements to TRS efficiency; solutions for direct communication between people with communication disabilities and other telephone users; and the effectiveness, efficiency, and consumer response to current and future approaches for delivering TRS. At the FCC's request, the Health FFRDC developed a Video Access Technology Reference Platform (VATRP) in support of the ACE program. This platform was developed in accordance with the Relay User Equipment (RUE) Specification to serve as a standards-based test platform for interoperability.

1.2 Purpose and Scope

This document presents an overview of the VATRP's release history, features, installation and user guides, and test cases.

2. Release Notes

2.1 Release History

Table 1 describes the version history of the VATRP. The v0.0.75 Preview release coincided with finalizing the RUE Specification. The v0.0.76 Patch was released in preparation for the Video Relay Services (VRS) Session Initiation Protocol (SIP) Interoperability Virtual Conference, which was held November 12–16, 2018. The v0.1 Release Candidate precedes the January v1.0 release.

Table 1. VATRP Version History

Version	Release Date	Enhancements / Features Introduced
0.0.75 Preview	October 11, 2018	<ul style="list-style-type: none"> • VATRP Preview released to VRS Providers and the FCC • Used for testing of registration • Enabled use of anonymous calls • Enabled Content Data Network (CDN) Endpoint configuration through User Interface (UI) • Enabled xCard Endpoint configuration through UI
0.0.76 Patch	November 8, 2018	<ul style="list-style-type: none"> • VATRP Preview patch for registration issues • Includes support for using a configuration file for registration • Additional features for testing include calling, mute, privacy, and Real-Time Text (RTT) • User ID added as registration input parameter • Enabled Call-Info and Geolocation endpoint configuration through UI
0.1.0 Release Candidate	December 5, 2018	<ul style="list-style-type: none"> • One-stage dial-around • Session Initiation Protocol (SIP) over Transport Layer Security (TLS) encryption • Changed application logo from “ACE” to “VATRP” • Registration patches for Proxy server and configurable port
1.0 Release	January 2, 2019	<ul style="list-style-type: none"> • Adaptive Rate Control • Patch for Datagram Transport Layer Security (DTLS) support and for calls placed using an unsupported encryption • Additional test cases in the test plan
1.1 Release	July 31, 2019	<ul style="list-style-type: none"> • NAT Traversal • Video quality features (PLI [Picture Loss Indication], PFU [Picture Fast Update], FIR [Full Intra-Request]) • Patches for DTLS, xCard, anonymous calls, config file loading • Registration to an outbound proxy

2.2 Known Issues

Table 2 describes the known issues as of this release (v1.1). The issue ID corresponds to the ID listed in the “FCC VATRP” Jira workspace. For example, ID 5 in Table 2 corresponds to “VATRP-5” in the Jira workspace.

Table 2. VATRP Known Issues

ID	Description
1	Audio and video codec settings do not persist between sessions.
15	VATRP is unable to connect to some Providers' videomail servers.
17	Call history is not saved when logging into a different device.
18	The timestamp for call duration in call history is not correct.
19	The "Provider" field box is blank when adding a new contact.
21	Some of the text to be displayed on the settings summary tab is cut off when clicking “View TSS.”
23	SIP Encryption checkbox in General settings is disabled.
24	Media encryption checkbox is not configurable from login window and does not persist between sessions.
25	Some call metrics in the Info icon view are not accurately reported.
26	vCard is presented as an option for the local file import/export for xCard.
29	Dialpad disappears after holding down a key for DTMF transmit for more than 2 seconds; for an 8-second transmit, nothing is sent.
30	RTT sometimes uses a different rtpmap than what is negotiated.
36	VATRP crash on some outbound calls during SIP RINGING event.
38	NAT Traversal can only be enabled from the settings menu, not from the configuration file.

2.3 Resolved Issues

Table 3 describes the issues that have been resolved since the v1.0 release.

Table 3. VATRP Resolved Issues

ID	Description
13	Selected media encryption not displayed in settings.
16	User needs to add leading 1 to 10-d number for logging in/dialing.
20	There are several feedback forms that will freeze the application when the user clicks on “Send.”
22	VATRP does not properly handle registration to an outbound proxy.
27	xCard server import requires user to manually enter credentials, is not optional, and does not try to retrieve credentials from the configuration.
28	VATRP freezes after xCard server import.
31	Transmission Control Protocol (TCP) and TLS port are not configurable.

ID	Description
33	VATRP crash when TLS and media encryption are selected.
35	Auth-ID and username are not displayed correctly if loaded in from a config.
37	VATRP crash on loading in config file with Message Waiting Indicator (MWI) Uniform Resource Identifier (URI).
32	The user agent field does not include any VATRP version information.

3. Installation Guide

This section provides a quick installation guide with an installer file and instructions for building and installing from the VATRP source code. In both installations, the VATRP must be installed on a Windows 10 platform.

The minimum requirements for VATRP installation consist of the following:

- Windows 10.X Operating System (OS)
- Webcam
- Microphone
- Microsoft Visual C++ 2013 Redistributable
- Microsoft Visual Studio Community 2015 Update 3 (for building from source code)

3.1 Quick Installation

Download the VATRP.msi file on a Windows 10 machine. Open the file, using Windows Installer as the default application. The VATRP Setup Wizard will appear as shown in Figure 1.

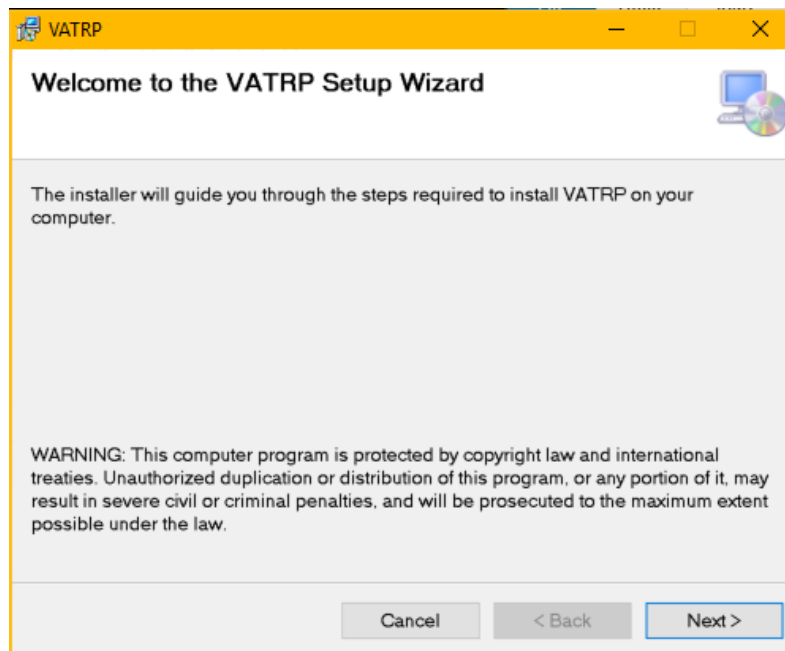


Figure 1. Screenshot of VATRP Setup Wizard

Click “Next” and then click through the prompts to install the VATRP. The VATRP Setup Wizard can be closed after successful installation. The VATRP can be opened via the shortcut in the start menu or by running ACE.exe from the directory chosen during the installation.

3.2 Installation from Source Code

Building from the source code requires Windows 10, Microsoft Visual Studio 2015 Update 3, and Git Bash or a Git client for Windows.

3.2.1 Installing Microsoft Visual Studio

When installing the Microsoft Visual Studio IDE, navigate to the “Older Versions” sections of the download page and then continue with Visual Studio Community 2015 Update 3.

Downloading the IDE may require creation of a Microsoft 360 account. During the installation process, select a custom install.

On the following page, check the box that selects all the available installation options and then de-select the C++ package. The installation may take several hours to complete.

The VATRP has been provisioned with an installer project that simplifies the process of installing the endpoint client device. Execute the following steps to install Microsoft Visual Studio:

1. Run Visual Studio as Administrator and select the “Extensions and Updates” option from the Tools dropdown.
2. Search 'installer' while in the online section.
3. Download and install Microsoft Visual Studio 2015 Installer Projects.
4. Close the running instance of Visual Studio and run the VSI_bundle.exe that was just downloaded.

3.2.2 Building the VATRP

Once Visual Studio has been installed and this repository has been cloned, take the following steps to build the VATRP:

1. Open the VATRP.sln file within the IDE.
2. Open the solution folder and right-click the VATRP solution.
3. Clean and rebuild the application before running it for the first time.

By default, the VATRP App project should already be selected as the default project to run. The navigation bar at the top of Visual Studio contains a green “Play” arrow icon that, when clicked, will build and run the application in debug mode. To run the application outside this mode, press Ctrl F5 as a short cut.

3.2.2.1 Reference Errors

If there are any issues regarding an assembly reference to Windows Devices or the IAsync type when building the project solution for the first time, then complete the following:

1. Navigate to the “Uninstall a Program” window from the Start menu.
2. Select “Microsoft Visual Studio Community 2015” and click “Change.”
3. Install the Windows 10 SDK.

4. Open the VATRP.App project in Visual Studio.
5. Find the References item under the VATRP.App Project.
6. Right-click and select “Add reference”.
7. Select the option to Browse.
8. In the Browse popup, select the following file: C:\Program Files (x86)\Windows Kits\10\UnionMetadata\Windows.md or Windows.winmd.
9. Make sure the Windows.md or Windows.winmd reference file is checked off, then click “OK”.
10. Clean and rebuild the application. Any reference errors should be resolved.

4. User Guide

The following subsections describe how to register the VATRP to a SIP server and interact with its features.

4.1 Registration

When launching the VATRP, a login screen appears as shown in Figure 2. The user can choose to provide the relevant information in the UI text fields or upload a JSON (JavaScript Object Notation) configuration file that populates the fields found in the JSON file.

If the Provider is not listed under the dropdown, select “Custom” and enter the fully qualified domain name (FQDN) in the Server field. The username and the password must be entered. If needed, the optional fields for auth-id, port and outbound proxy can be filled out as well.

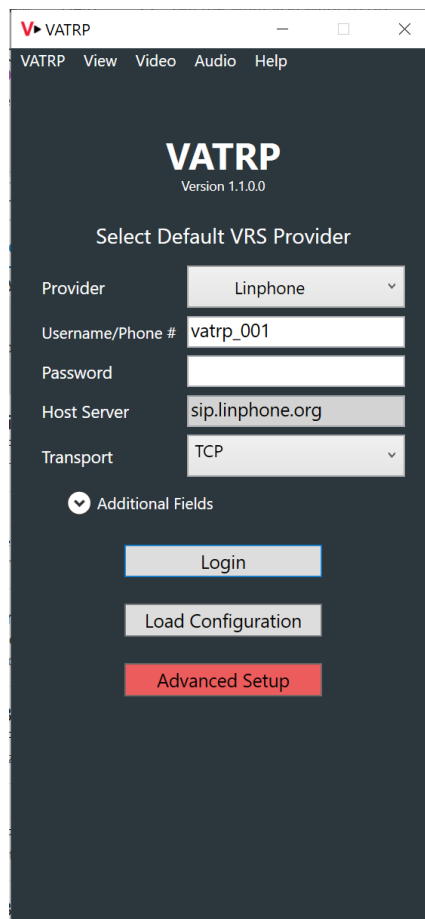
The screenshot shows the VATRP login interface. At the top, there's a header bar with the VATRP logo and version 1.1.0.0. Below this, a menu bar contains 'VATRP', 'View', 'Video', 'Audio', and 'Help'. The main content area is titled 'Select Default VRS Provider'. It features a form with the following fields: 'Provider' (a dropdown menu currently showing 'Linphone'), 'Username/Phone #' (a text field containing 'vatrp_001'), 'Password' (an empty text field), 'Host Server' (a text field containing 'sip.linphone.org'), and 'Transport' (a dropdown menu currently showing 'TCP'). Below these fields is a section labeled 'Additional Fields' with a downward arrow icon. At the bottom of the form are three buttons: 'Login' (a light blue button), 'Load Configuration' (a light gray button), and 'Advanced Setup' (a red button).

Figure 2. Screenshot of VATRP Login Screen

Selecting the “Advanced Setup” button can open the Settings window. In the Settings window, navigate to the Account tab. Several fields can be modified in this window, including the CDN URI, which can import the list of Providers.

To populate the “Provider” dropdown menu, go to the CDN URI field and place a URI that references a JSON document containing a list of Providers. If a configuration file was loaded, the Settings window should reflect the loaded content. Many of the fields in the Settings menu will remain unalterable and only activate once the login process has been completed.

After populating all the desired fields in the login screen, click “Login” to proceed to the VATRP main window depicted in Figure 3.

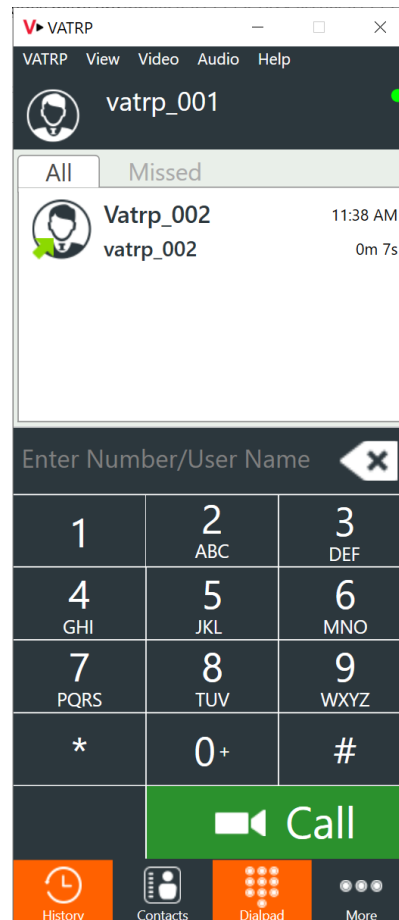


Figure 3. Screenshot of VATRP Main Window

The state of the registration attempt can be determined by the circular status indicator at the top right of the application. Table 4 lists the possible states. Note that even in a failed registration where the user reaches the main window, the user will not be able to make or receive calls.

Table 4. Registration Statuses

Color	Status
Green	Successful
Red	Failed
Gray	In Progress

4.2 Placing a Call

To place a call, select the dialpad tool from the navigation menu at the bottom of the application's display, enter a contact's phone number, and click "Call." If the callee answers, an on-screen menu will appear allowing for use of the VATRP's call features. Figure 4 presents a view of the VATRP when in a call. The following features are displayed from the viewer's left to right in the grayed out overlay buttons:

- Video Privacy
- Microphone Mute
- Audio Mute
- Dual-Tone Multi-Frequency (DTMF) Dialpad
- Real-Time Text
- Pause Call

An "End Call" button appears at the bottom of the video window (and below the overlay buttons).

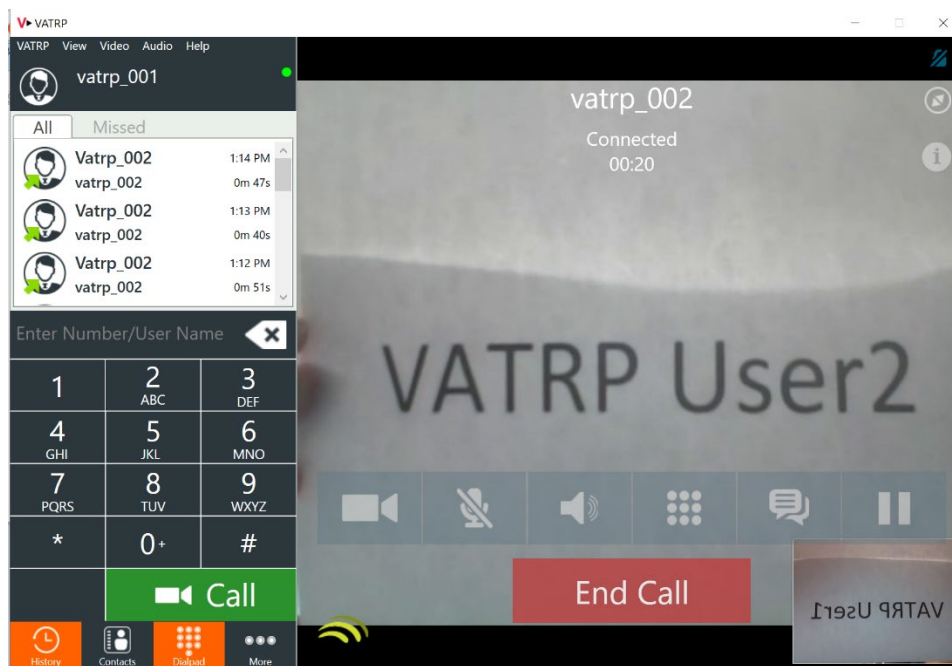


Figure 4. Screenshot of Call View

Note that depending on the laptop's configuration, firewall may need to be disabled in order to place a call.

4.2.1 Placing an Encrypted Call

After registering successfully, navigate to "More", then "Settings", and then "Summary." Enter the password in "Show Advanced." Click the "Advanced" tab and then scroll to the "Media

Encryption” pull-down menu. Click and select “Encrypted (DTLS).” This action will lead to one of the following two results:

- If a file called “linphone-dtls-default-identity.pem” exists within the same directory as the VATRP.exe, “Encrypted (DTLS)” will be enabled successfully. No further actions will be required.

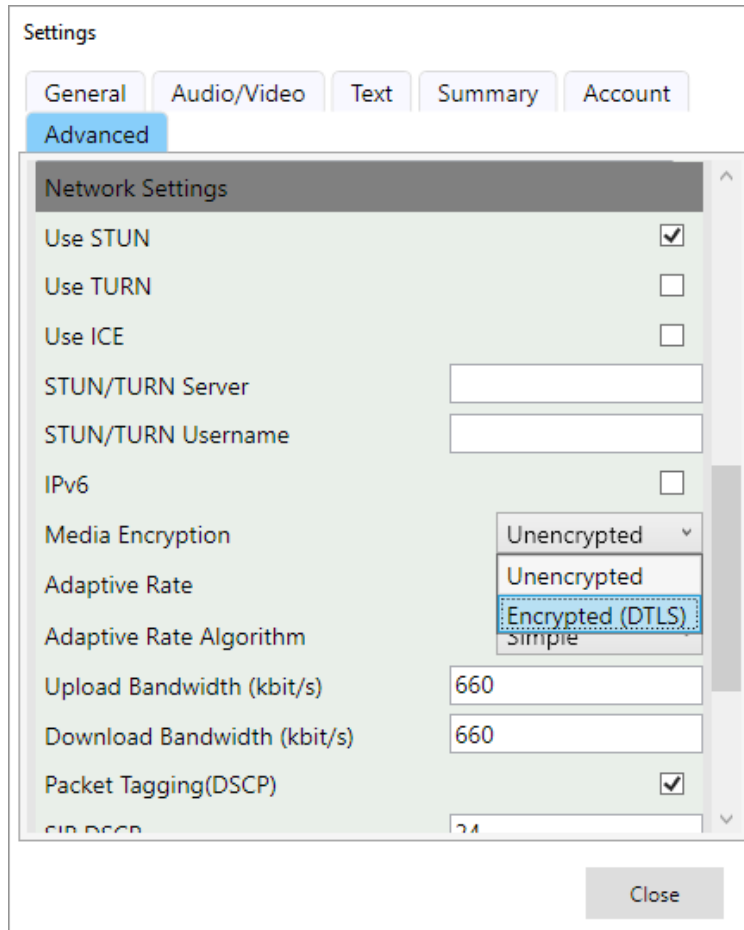


Figure 5. Enabling Encryption Using DTLS

- If the file “linphone-dtls-default-identity.pem” does not exist or is not located within the same directory as the VATRP.exe, a warning dialog will appear to indicate the file is missing and the call will be configured as unencrypted. If an unencrypted call is not feasible, a potential solution is to manually generate the “linphone-dtls-default-identity.pem” file and put it into the same directory as VATRP.exe. To generate a new “.pem” file:
 - Navigate to <https://www.ssh.com/ssh/putty/windows/puttygen> to install PuTTY and generate a new DTLS encryption key. Some important notes:
 - ♦ After the key is generated, do not provide a passphrase for the generated key.

- After the key is generated, export the generated key into OpenSSH format and save it as “linphone-dtls-default-identity.pem” in the same directory as VATRP.exe.

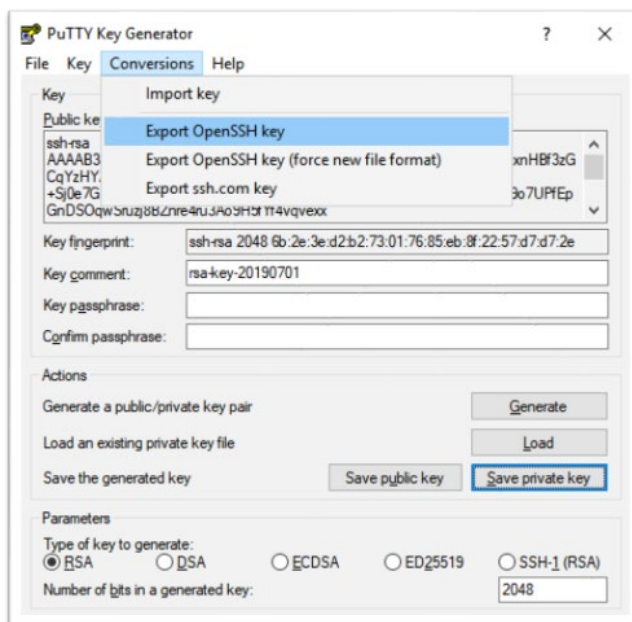


Figure 6. Generate and Export a New “linphone-dtls-default-identity.pem”

- Open the “linphone-dtls-default-identity.pem” using a regular text editor. Visually check that the file only has the private key section.
- Next, located and open a file called “rootca.pem” from where the VATRP executable is located. If the installer is used to install VATRP, both the VATRP executable and the “rootca.pem” should be located in “C:\Program Files (x86)\The MITRE Corporation\VATRP”
- Copy and append a certificate from “rootca.pem” (only copy from “-----BEGIN CERTIFICATE-----” to “-----END CERTIFICATE-----”) to the end of the “linphone-dtls-default-identity.pem”
- Return to the settings menu to re-enable media encryption.
- If the file “linphone-dtls-default-identity.pem” exists but does is not properly formatted, a warning dialog will appear when enabling media encryption. This is likely due to a missing certificate section in the pem file. Follow the instructions listed in the previous bullet points involving rootca.pem. After adding the certificate to the pem file, re-enable media encryption in the settings menu.

4.3 Features

4.3.1 Real-Time Text

When a user has selected the RTT feature from the on-screen menu bar, a new dialog box attaches to the right side of the video stream view as shown in Figure 5. As a message is typed, a

character-by-character stream is sent to the other user. When the ENTER key or SEND button has been clicked, the message remains in the dialog view.

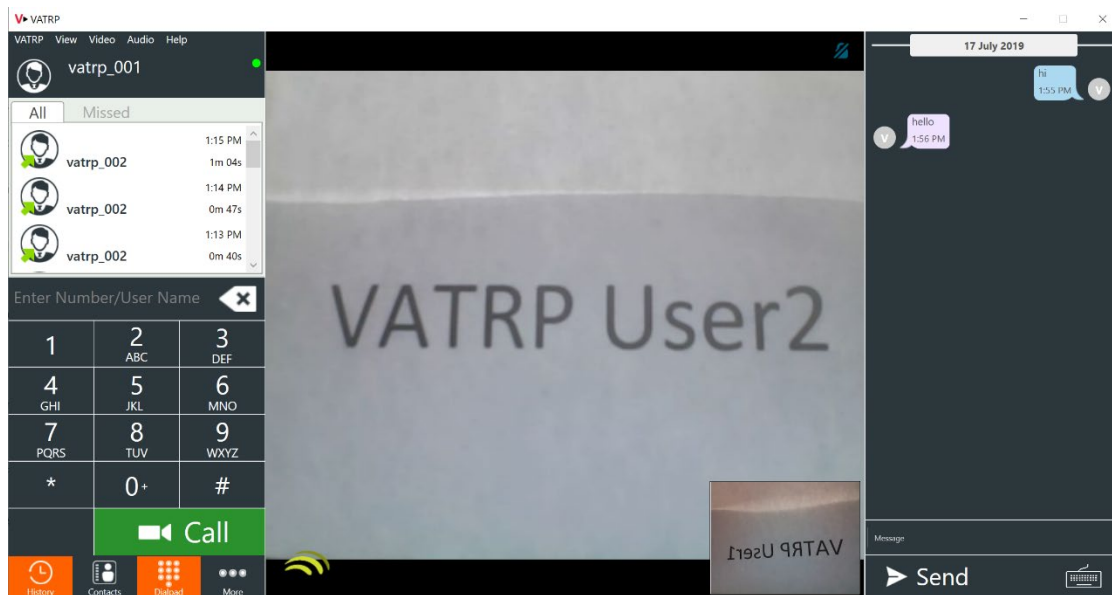


Figure 7. Screenshot of Call View with Chat

To mute RTT, click the keyboard icon on the bottom right side of the RTT dialog. This hides the message bar and prevents the user from sending additional messages or text characters until RTT is unmuted.

4.3.2 Contacts

To view the current list of saved contacts that can be used to place calls, select the “Contacts” option in the bottom pane of the main window. To manually add a new contact, select the “+” icon near the top right of the contacts window. This will open a new window where the new contact’s information can be inputted and saved.

Contacts can be imported by selecting the down-arrow icon near the top right of the contacts window. To import contacts, one of two options must be selected:

1. **Import from a remote URI to the local machine through a HTTPS web request.** This URI can be set through the Settings window under the Account tab.
2. **Import from the local file system.** Either a vCard file or xCard (Extensible Markup Language [XML]) formatted list of contacts can be selected.

If there are contacts present in the VATRTP account, they can be exported like the contact import options described. This feature can be used by selecting the up-arrow icon near the top right of the contacts window.

4.3.3 Message Waiting Indicator

The VATRP has the ability to subscribe to videomail notifications from a server specified by the Video Mail URI in the account settings. If the user's videomail inbox contains media that has not been viewed, a status indicator appears in the settings menu tab, alerting the user to the total number of outstanding messages. Viewing or removing the unviewed messages will remove the MWI mailbox notification. Videomail retrieval in the VATRP is currently in development.

5. VATRP Test Plan

This section contains test cases to measure interoperability with the VATRP and assess RUE Specification compliance. While all tests have user-based verification, some also involve analyzing packet captures or REST calls. For tests that require analyzing packet captures, Wireshark¹ needs to be installed and run according to the test case instructions. All Graphical User Interface (GUI)-related actions and results are based on the VATRP as User 1. For any testing that involves a non-VATRP endpoint as User 2, the tester should find the appropriate place on the endpoint's GUI to complete the test case.

For each Provider, test calls will be placed between the VATRP registered to that Provider's server and the other VRS endpoints. The results will be documented in two matrices—a Requirements Traceability Matrix for tests involving multiple calls and a Requirements Traceability Matrix for tests conducted once per Provider. Figure 6 and Figure 7 show examples of these matrices.

There will be a unique matrix for Figure 6 corresponding to each of the VRS Providers, namely, Convo, Global, Purple, Sorenson, and ZVRS. The matrix in Figure 7 will be used for all Providers. Each set of requirements in Figure 6 will be tested against all Provider endpoints over each of the Provider server environments, unless designated as "Not Tested." Each set of requirements in Figure 7 will be tested once per Provider on the VATRP registered to the designated Provider.

¹ <https://www.wireshark.org/faq.html>

VATRP TRACEABILITY MATRIX: Tests Involving Multiple Calls		<div><div><div><div><div><div></div><div>FEDERAL COMMUNICATIONS COMMISSION</div><div>USA</div></div></div><div><div></div><div>FC</div><div></div></div></div></div></div>																																Convo					Global				Purple							Sorenson					ZVRS					
		Provider Endpoint																																																										
		Convo Softphone (iOS)	Convo Softphone (Android)	Convo Softphone (Mac/OSX)	Convo Softphone (PC/ Windows 10)	Convo VATRP Softphone (PC/Windows 10)	Global Softphone (PC/Windows 10)	Global Softphone (iOS)	Global Softphone (Android)	Global VATRP Softphone (PC/Windows 10)	Purple Smart VP (Desktop)	Purple P70 (Desktop)	Purple P3 Softphone (iOS)	Purple P3 Softphone (Android)	Purple P3 Softphone (Mac/OSX)	Purple P3 Softphone (PC/Windows 10)	Purple VATRP Softphone (PC/Windows 10)	Sorenson nTouch VP (Desktop)	Sorenson nTouch VP2 (Desktop)	Sorenson nTouch Softphone (iOS)	Sorenson nTouch Softphone (Android)	Sorenson nTouch Softphone (Mac/OSX)	Sorenson nTouch Softphone (PC/Windows 10)	Sorenson VATRP Softphone (PC/Windows 10)	ZVRS Z20 - Cisco E20 (Desktop)	ZVRS Z5 Softphone (iOS)	ZVRS Z5 Softphone (Android)	ZVRS i3	ZVRS Z5 Softphone (Mac/OSX)	ZVRS Z5 Softphone (PC/Windows 10)	ZVRS Z70 - Cisco (Desktop)	ZVRS VATRP Softphone (PC/Windows 10)																												
VATRP Test Case for Provider: _____		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31																												
5.3.1 - Call Quality (Video - Effective ASL)	1																																																											
5.3.1 - Call Quality (Audio - Comprehension)	2																																																											
5.3.2 - Media Encryption	3																																																											
5.3.3 - Video Privacy	4																																																											
5.3.3 - Audio Mute	5																																																											
5.3.4 - DTMF Transfer*	6																																																											
5.3.5 - Real-Time Text (RTT)*	7																																																											
5.3.6 - Pause/Resume Call	8																																																											
5.4.1 - Multiple Registered RUEs to One Account*	9																																																											
5.4.2 - Anonymous Call	10																																																											
5.7.1 - One-stage Dial-Around	11																																																											

Test Case Legend:

*: Required if the Provider supports the functionality on at least one endpoint
All other test cases are required.

Results Legend:


Passed RUE Test Requirement

Passed with caveats - Video or Audio Quality Issues (or other specified issue)

Failed RUE Test Requirement

Not Tested

Figure 8. VATRP Traceability Matrix for Tests Involving Multiple Calls

VATRP TRACEABILITY MATRIX: Tests Conducted Once Per Provider						
		Provider				
			Convo	Global	Purple	Sorenson
VATRP Test Case			1	2	3	4
5.1.1 - Registration	1					
5.1.2 - SIP over TLS Encryption	2					
5.2.1 - Geolocation Transfer	3					
5.2.2 - Contact Info Transfer	4					
5.5.2 - Message Waiting Indicator (MWI)*	5					
5.6.1 - Import/Export Contact List via xCard file format	6					
5.6.2 - Import/Export Contact List via CardDAV Server*	7					
5.8 - Emergency Call Handling	8					

Test Case Legend:

*: Required if the Provider supports the functionality on at least one endpoint
 All other test cases are required.

Results Legend:

Passed RUE Test Requirement
 Passed with caveats - Video or Audio Quality Issues (or other specified issue)
 Failed RUE Test Requirement
 Not Tested

Figure 9. VATRP Traceability Matrix for Tests Conducted Once Per Provider

Many of the tests require the user to be in a call scenario; therefore, Table 5 presents the typical call procedure.

Table 5. Point-to-Point Call Procedure

Step	Action	Expected Result
1	User 1 navigates to call screen.	User 1 should see input box for phone number or SIP URI.
2	User 1 inputs phone number of User 2 in the input box and clicks a button to place a call.	User 1 should see or hear ring-back and visual feedback describing connection status information.
3	User 2 sees visual and/or audio notification of an incoming call and clicks button to receive the call.	User 1 and User 2 should see connection status information associated with the call connection.
4	Both users interact for 2 minutes.	Video and audio quality should be acceptable for duration of call.
5	User 1 hangs up.	Verify that the call terminates correctly from both ends.

The following subsections describe test cases for each of the outlined VATRP Test Areas.

5.1 Registration

This subsection contains test cases for registering and using TLS encryption.

5.1.1 Registration Test

The Provider has a choice of registering with the fields in the login screen or by uploading a configuration file. Table 6 presents a procedure for testing registration by either method. The registration test must be performed once for each Provider on the VATRP only.

Table 6. Registration Test

Step	Action	Expected Result
1	User 1 opens the VATRP application.	The VATRP login screen appears.
2	(For configuration file. If using UI only, skip to Step 4.) User 1 clicks "Load Configuration."	A window pops up that allows the user to select a file.
3	User 1 selects a properly formatted JSON configuration file and clicks "Open."	The file selection window closes. For fields that are present in the configuration file and the UI, their values are populated in the UI.

Step	Action	Expected Result
4	User 1 enters information in any necessary login fields that were not populated by the configuration file. Then the user clicks "Login."	The VATRP main window appears, and the login status circle changes from gray to green.
5	(Ongoing) Periodically check the status circle during other tests.	The login status circle should remain green to indicate that User 1 is still logged in.

5.1.2 SIP over TLS Encryption

Table 7 presents the test case for SIP over TLS encryption. This test must be performed once per Provider on the VATRP only.

Table 7. SIP over TLS Encryption Test

Step	Action	Expected Result
1	User 1 starts a Wireshark capture.	Wireshark captures the packet flow for the VATRP endpoint registering to the Provider server.
2	User 1 completes registration as described in the registration test case, choosing TLS for Transport.	Registration takes User 1 to the VATRP main window and is successful.
3	User 1 waits until the registration status indicator turns green and then ends the Wireshark capture.	In the Wireshark capture, the last (most recent) "TLS SERVER HELLO" message before the "REGISTER" message should show version 1.2 or higher, with a minimum cipher suite of TLS_RSA_WITH_AES_256_CBC_SHA256.

5.2 Geolocation and Contact Information

The geolocation and contact information test is conducted once per Provider on the VATRP only. Table 8 describes the test case.

Table 8. Geolocation and Contact Information Test

Step	Action	Expected Result
1	User 1 opens the VATRP and navigates to "Advanced Setup," then to "Account," to enter a Geolocation URI.	The Geolocation URI is saved in the Advanced Setup menu. A pop-up window appears asking the user if they want geolocation to be sent during registration.
2	User 1 selects the "Yes" button and then clicks "Close" on the Settings menu.	The flag to send Geolocation during registration is set to true and User 1 returns to the login screen.
3	User 1 starts a Wireshark capture.	Wireshark captures the packet flow for the VATRP endpoint registering to the Provider server.

Step	Action	Expected Result
4	User 1 completes registration as described in the registration test case.	Registration takes User 1 to the VATRP main window and is successful.
5	User 1 waits until the registration status indicator turns green and then ends the Wireshark capture.	In the Wireshark capture, the last (most recent) the "REGISTER" message should contain a Geolocation header with the Geolocation URI provided in the Advanced Setup menu. In addition, the message should contain a Contact header with the correct contact information for User 1.

5.3 Current Call Features

The current call feature tests include tests for call quality, media encryption, audio mute, video privacy, DTMF, RTT, and call on hold. The following subsections provide a description of these test procedures.

5.3.1 Call Quality

The call quality tests include subjective measures of video and audio quality as outlined in Table 9 and Table 10. The tests must be conducted on all endpoints.

Table 9. Subjective Video Quality Test Criteria

Criterion	Video Quality Criteria
1	Visible: The tester reports whether the other endpoint sees the incoming video (e.g., not a black or green screen).
2	Conversational: The tester reports whether video quality is acceptable for an ASL conversation.
3	Blurry / Pixelated: The tester reports any instances where the video is blurry, blocky, or pixelated at any point during the call.
4	Stutter / Stalls: The tester reports any video stutter or stalls, and the maximum delay effect observed.
5	Frame Rate: The tester reports the frame rate.

Table 10. Subjective Audio Quality Test Criteria

Criterion	Audio Quality Criteria
1	Audible: The tester reports whether the other endpoint hears the incoming audio.
2	Clear: The tester reports any noticeable distortions to the audio or echo.
3	Timing: The tester reports any significant latency to the audio stream and whether the audio appears in sync with the video.

Criterion	Audio Quality Criteria
4	Dropouts: The tester reports any dropouts in the audio.
5	Background noise: The tester reports whether background noise (loud intermittent or white noise) negatively affects the ability to hear the other person clearly.

5.3.2 Media Encryption

Table 11 describes the test for cases media encryption with Secure Real-time Transport Protocol (SRTP) and Secure RTP Control Protocol (SRTCP). Media encryption tests shall be conducted on all endpoints. Note that while the RUE Specification requires media encryption, the VATRP is also capable of completing calls without media encryption to maintain backward compatibility. This test requires encryption to be enabled on the VATRP.

Table 11. Media Encryption Test

Step	Action	Expected Result
1	After successfully registering with the VATRP, User 1 navigates to the Settings, then “Advanced Setup,” to the “Media Encryption” option. Once there, the user can enable the encryption.	The encryption checkbox is checked (enabled).
2	User 1 starts a packet capture in Wireshark and initiates a call using the Point-to-Point Call Procedure outlined in Table 5.	Call connects. Both User 1 and User 2 can communicate visually and by voice.
3	User 1 ends the Wireshark capture and navigates to Statistics, and then chooses Flow Graph.	Information about RTP packets is NOT displayed (information such as “Invite, BYE, and RTP Events cannot be observed in the flow graph).

5.3.3 Audio Mute and Video Privacy

Table 12 describes the test cases for audio mute and video privacy. Mute and privacy tests shall be conducted on all endpoints.

Table 12. Audio Mute and Video Privacy Test

Step	Action	Expected Result
1	User 1 initiates a call using the Point-to-Point Call Procedure.	Call connects. Both User 1 and User 2 can communicate visually and by voice.
2	User 1 hits the “Privacy” button.	User 2’s device indicates that User 1 is in privacy mode. User 2 cannot see User 1’s video stream but can still hear User 1’s audio stream.
3	User 1 turns off the Privacy option.	Call resumes normally with two-way video.

Step	Action	Expected Result
4	User 1 hits the microphone “Mute” button.	User 2 can no longer hear audio from User 1’s device but can still see User 1’s video stream. The User 2 device may or may not indicate that the remote audio is muted.
5	User 1 turns off the Mute option.	Both parties are again able to communicate verbally.
6	Switch sides and try again. (User 2 initiates privacy and mute options.)	Results should be the same as those in Steps 2 through 5, with the user switched.

5.3.4 Dual-Tone Multi-Frequency

Table 13 presents the test case for DTMF. The DTMF test results for VATRP compliance are only measured in VATRP-to-VATRP tests. Additional DTMF tests with other VRS endpoints are conducted as part of a general interoperability survey but will not impact compliance.

Table 13. DTMF Test

Step	Action	Expected Result
1	User 1 starts a packet capture in Wireshark and initiates a call using the Point-to-Point Call Procedure.	Call connects. Both User 1 and User 2 can communicate visually and by voice.
2	User 1 clicks the DTMF dialpad button.	A dialpad appears on the screen.
3	User 1 presses 0-9, *, and # on the dialpad for short transmissions. Then User 1 presses 0-9, *, and # on the dialpad for long transmissions.	Audio may be transmitted from User 1 to User 2 but is not required for the DTMF telephony event. There may be no noticeable change for the user.
4	Switch sides and try again. (User 2 sends DTMF.)	Results should be the same as those in Steps 2 and 3, with the user switched.
5	User 1 ends the Wireshark capture and navigates to Statistics, and then chooses Flow Graph.	The DTMF tones appear in the flow graph as “RTP (telephony event) DTMF” followed by the number that was pressed.

5.3.5 Real-Time Text

Table 14 contains the test cases for RTT and RTT mute. The RTT tests are conducted on all endpoints that support RTT.

Table 14. RTT Test

Step	Action	Expected Result
1	User 1 initiates a call using the Point-to-Point Call Procedure.	Call connects. Both User 1 and User 2 can communicate visually and by voice.
2	User 1 clicks the chat icon.	An RTT chat tab appears next to the video.

Step	Action	Expected Result
3	User 1 types a message but does not click "Send."	User 2 can see the message coming in, character by character, with less than a 1-second delay.
4	User 1 and User 2 type messages at the same time. (Note: At the end of this step, User 2 may stop typing.)	Each user sees the message from the other user coming in, character by character, with less than a 1-second delay.
5	User 1 hits "Enter" and starts to type a new message.	User 2 sees the first message fixed on the screen with no more changes, and a second message window with the new message coming in character by character, with less than a 1-second delay.
6	User 1 clicks the keyboard icon to initiate RTT mute.	User 1 cannot type anything new. User 2 does not see any incoming RTT from User 1.
7	User 1 clicks the keyboard icon to unmute RTT, and then begins typing a message.	User 2 sees the incoming message from User 1, character by character, with less than a 1-second delay.
8	Switch sides and try again. (User 2 repeats RTT test.)	Results should be the same as those in Steps 2 through 7, with the user switched.

5.3.6 Pause Call

Table 15 presents the pause call test. This test is conducted on all endpoints.

Table 15. Pause Call Test

Step	Action	Expected Result
1	User 1 initiates a call using the Point-to-Point Call Procedure.	Call connects. Both User 1 and User 2 can communicate visually and by voice.
2	Both users interact for 1 minute.	Video and audio quality should be acceptable for duration of call.
3	User 1 clicks the pause button to pause the call for 30 seconds and then resumes the call.	While paused, User 1 sees the pause sign in the video window. User 2 sees a frozen video of the last frame and receives no audio. When the call resumes, video and audio resume as in a typical call scenario.
4	User 2 pauses the call for 30 seconds and then resumes the call.	Video and audio should cease while paused, then continue when the call resumes.

5.4 Additional Call Features

5.4.1 Multiple Registered RUEs

The test case for multiple registered RUEs involves two VATRP endpoints and one additional endpoint registered to the same account that receives a call from another VATRP endpoint.

Table 16 describes this test case. This test is conducted on all endpoints that support multiple registrations.

Table 16. Multiple Registered RUEs Test

Step	Action	Expected Result
1	User 1 registers on the VATRP to a unique account. Users 2 and 3, on the VATRP, and User 4, on another endpoint, all register to the same account.	Users 2, 3, and 4 can successfully register and remain registered.
2	User 1, on the VATRP, places a call to the phone number shared by Users 2, 3, and 4.	Users 2, 3, and 4 all receive audio and/or visual notification of an incoming call.
3	User 2 answers the call.	The call is established correctly between User 1 and User 2. User 3 and User 4's endpoints stop ringing.
4	Repeat steps 2 and 3 twice, with the remaining Users (3 and 4) taking turns answering the call.	The same expected behavior should occur but with a different endpoint answering.
5	Users 2 through 4 initiate a call to User 1.	The call is established correctly between Users 2 through 4 and User 1.
6	User 4 de-registers. Repeat steps 2 through 5, with only Users 2 and 3 registered.	The expected behavior of steps 2 through 5 should occur for Users 2 and 3.
7	User 3 de-registers. User 1 calls User 2.	The call is established correctly between User 1 and User 2.
8	User 2 calls User 1.	The call is established correctly between User 1 and User 2.

5.4.2 Anonymous Calls

Table 17 describes the test case for anonymous calls. The anonymous call tests are conducted with the VATRP placing outbound anonymous calls to all endpoints. The non-VATRP endpoints will not place outbound anonymous calls for this test case.

Table 17. Anonymous Call Test

Step	Action	Expected Result
1	User 1 enables anonymity. (In the VATRP, navigate to "Settings," then "General," and then check the "Privacy" box.)	User 1 should see that Privacy is enabled in the Settings menu.
2	User 1 starts a Wireshark capture of the call. User 1 inputs phone number of User 2 in the input box and clicks a button to place a call.	User 1 should see or hear ring-back or visual feedback describing connection status information.
3	User 2 receives the call.	User 2 sees visual and/or audio notification of an incoming call, with "Anonymous" displayed in place of the caller ID or phone number.

Step	Action	Expected Result
4	Switch sides and try again. (User 2 repeats the anonymous call test.)	Results should be the same as those in Steps 1 through 3, with the user switched.
5	User 1 ends the Wireshark capture and finds the SIP INVITE message.	In the header of the SIP INVITE, the "From" header field should have ' "Anonymous" sip:anonymous@anonymous.invalid ' before the ";tag=...". User 1's ID and telephone number should not appear in any header field in the SIP INVITE.

5.5 Message Waiting Indicator

Table 18 presents the test case for leaving a videomail and then tracking the Message Waiting Indicator (MWI). MWI tests are conducted on the VATRP only for Providers where at least one client supports a videomail notification.

Table 18. Message Waiting Indicator Test

Step	Action	Expected Result
1	User 1 registers to the VATRP.	User 1 successfully registers and sees no messages waiting. If there are messages waiting, User 1 retrieves the messages so that the MWI disappears.
2	User 1 logs off and User 2 places a call to User 1.	User 2 leaves a videomail message by following the videomail Interactive Voice & Video Response (IVVR) presented to them.
3	User 1 logs back in.	User 1 sees the MWI displaying 1 message waiting.

5.6 Contact List Management

5.6.1 xCard

Table 19 presents the test procedure for xCard. This test is conducted once per Provider on the VATRP only. The User 2 mentioned in this test case must be another VATRP endpoint registered to the same Provider.

Table 19. xCard Test

Step	Action	Expected Result
1	User 1 navigates to Settings and then to Account and provides a Contacts URI that will upload an XML file containing User 2's contact information.	The contacts URI is successfully loaded in (the User can click "Close").

Step	Action	Expected Result
2	User 1 navigates to the Contacts tab and clicks the down-arrow icon for import.	User 1 sees a pop-up window with import options.
3	User 1 clicks “Yes” to import from the server.	User 1 sees the imported contacts in the contacts list.
4	User 1 places a call to one of the imported contacts, which is User 2.	User 1’s call to User 2 is successful.
5	User 1 navigates to the contact view and clicks the up-arrow icon for export.	User 1 sees a pop-up window with export options.
6	User 1 clicks “Yes” to export to the server.	The contacts are successfully exported, which can be verified by checking the XML file. All contacts in the imported file are correctly represented in the exported file.
7	User 1 opens Postman and creates a GET request for the exported contacts.	User 1 can use the response to verify that the contact export was successful.

5.6.2 CardDAV

The test case for CardDAV is in development.

5.7 One-Stage Dial-Around

Table 20 presents the test procedure for one-stage dial-around. This test is conducted once per Provider pair on the VATRP only, and only if both Providers have indicated that they support one-stage dial-around.

This test case requires the use of a Communication Assistant (CA) and a call to a non-VRS number.

Table 20. One-Stage Dial-Around

Step	Action	Expected Result
1	User configures the VATRP to place a dial-around call by selecting the dial-around Provider from the drop-down menu next to the call button.	The dial-around Provider is selected.
2	User initiates a dial-around call with a second Provider to a non-TRS number (e.g., the FCC IVR at 888 225-5322).	The test call completes to the non-VRS numbers and a CA from the second Provider interprets the call.
3	User repeats step 1, swapping first and second Providers.	The test call completes to the non-VRS numbers and a CA from the first Provider interprets the call.

5.8 Emergency Calls

The emergency calls test case is in development.

Acronyms

ACE	Accessible Communications for Everyone
ASL	American Sign Language
CA	Communication Assistant
CDN	Content Data Network
CMS	Centers for Medicare & Medicaid Services
DLL	Dynamic-Link Library
DTLS	Datagram Transport Layer Security
FCC	Federal Communications Commission
FFRDC	Federally Funded Research and Development Center
FIR	Full Intra Request
FQDN	Fully Qualified Domain Name
HHS	Department of Health and Human Services
HTTPS	HyperText Transport Protocol Secure
IDE	Integrated Development Environment
IP	Internet Protocol
IVVR	Interactive Video & Voice Response
JSON	JavaScript Object Notation
MWI	Message Waiting Indicator
NAT	Network Address Translation
OS	Operating System
PFU	Picture Fast Update
PLI	Picture Loss Indication
REST	Representational State Transfer
RFC	Request for Comment
RUE	Relay User Equipment
RTT	Real-Time Text
SDK	Software Development Kit
SDP	Session Description Protocol
SIP	Session Initiation Protocol

SRTP	Secure Real-Time Transport Protocol
STUN	Session Traversal Utilities for NAT
TCP	Transmission Control Protocol
UI	User Interface
URI	Uniform Resource Identifier
URL	Universal Resource Locator
VATRP	Video Access Technology Reference Platform
VRS	Video Relay Service
XML	Extensible Markup Language

Notice

This (software/technical data) was produced for the U. S. Government under Contract Number 75FMC18D0047, and is subject to Federal Acquisition Regulation Clause 52.227-14, Rights in Data-General.

No other use other than that granted to the U. S. Government, or to those acting on behalf of the U. S. Government under that Clause is authorized without the express written permission of The MITRE Corporation.

For further information, please contact The MITRE Corporation, Contracts Management Office, 7515 Colshire Drive, McLean, VA 22102-7539, (703) 983-6000.

© 2019 The MITRE Corporation. All rights reserved.