Figure 1: Caption added because VEP flow diagram was too complicated

Voice Encryption Protocol (VEP)

Written by: Andrew Kosakowski

Table of Contents

Index of Tables

Document Introduction

As of the time of publishing this document Voice Encryption Protocol (VEP) is a conceptual protocol that is being released for discussion and consideration for development. This protocol and related documentation is free for all uses, development, implementation, discussion, and/or dissemination as long as this document and this permission-set is attached to all derivative, non-derivative, and/or future works, discussions, development, solutions, implementations, dissemination, and/or all other uses. The document flow is designed to provide an introduction followed by deeper technical sections. The first section is an overview of VEP and how it is intended to operate. The first section will introduce the phone number standard that has been designed for VEP. The second section in the technical portion of this document is the assumptions section which will provide insights about what is a VEP responsibility versus the responsibility of another solution. The VEP components are discussed in the next major section and include the VEP Provider, VEP database, and VEP Clients. The following section discusses VEP implementation and usage. The final section is a wrap-up that discusses any remaining issues and provides a document summary.

Overview of VEP

VEP is a conceptual protocol that has been created as a direct result of the onslaught of privacy invasion issues that have been exacerbated by government and private enterprise surveillance, over zealous service providers, the proliferation and ease-of-use of eaves dropping equipment and software just to name a few reasons. The central implementation device in VEP is the VEP Provider which acts as a central encryption proxy for all access up updates to the VEP database, ensure non-repudiation of clients, and manages VEP Identities. The VEP database has two components, the “contacts” storage area and the “voice messages” storage area. The VEP client is a user-specific package that is provided directly from the VEP Provider. To initiate a call a user dials the recipient’s number, the VEP Client forwards the request to the VEP Provider, the VEP Provider verifies and authenticates the request then forwards the call to the recipient. If the recipient answers the call is initiated. If the recipient is unavailable the VEP Provider forwards the call to the VEP database where the voice message is stored.

VEP Phone Number Standard

The VEP phone number standard is a conceptual numbering standard that is being recommended in compliment of the VEP protocol. The VEP Phone number standard has over 18 quintillion possible number assignments. As the number of phone numbers any one entity may be required for assignment and the number of voice-capable devices increases there is a need for a more robust set of numbers that are assigned in a defined structure that will assist in facilitating non-repudiation, location verification, and privacy while also decreasing the effectiveness of robo-dialers and currnet voice-enabled attacks.

Format

A VEP Phone number is composed of four sets of 4-digit hexadecimal numbers separated by a dash ‘-’ (ex. 1D3A-0142-BADC-926E). This provides 18,446,744,073,709,551,616 (18 quintillion 446 quadrillion 744 trillion 73 billion 709 million 551 thousand 616) total possible numbers. This format has been chosen as it provides a compact way to achieve a large number of possible assignments.

Structure

The structure of a VEP phone number consists of 4 parts. The 1st digit in every number represents major spacial location. The number '1' is reserved for Earth and '0' is reserved for testing and non-production issues. The 2nd digit in the first set represents the major location such as continent, orbit, or moon. The 3rd and 4th digit in the first set indicate the minor geographic region within the major location. There are 256 possible assignments for minor geographic locations within each major geographic location. This provides nearly five assignments for every country in the most heavily divided continents; however, as populations are not evenly distributed between nations it may be likely the assignments will be distributed in relation to population dispersal and not national boundaries. The 1st and 2nd digit in the second set are reserved to indicate customer component. The remaining 2 digits in the second set and final two sets are reserved for customer assignment. This permits 4,294,,967,296 (4 billion 294 million 967 thousand 296) possible numbers for every customer component in each minor location for every major location at each space site.

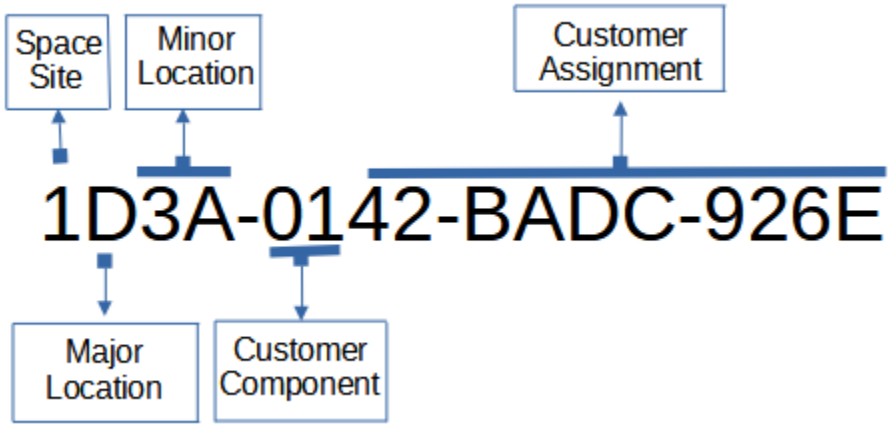

Figure 2: Phone Number Structure

Reserved Assignments

The tables below provide the currently recommended assignments for the four number assignment components: Space Site, Major Location, Minor Location, and Customer Component.

Table 1: Space Site Number Assignments

Assignment	Site Name
0	Reserved for research and non production use
1	Earth and earth orbit areas
2	Mars
3 through F	Held for future assignment

The following table has been created as an example list of Earth's Major locations and which assignments may be used. Take note that some of these proposed assignments would only be useful for future assignments as technological capabilities improve. These assignments are suggestions and are not mandatory for use at this time.

Table 2: Major Location Number Assignments

Assignment	Major Location
0	Earth's Moon
1	Exosphere
2	Thermosphere
3	Mesosphere
4	Mesosphere
5	Stratosphere
6	Africa
7	Antarctica
8	Asia
9	Australia
A	Europe
B	North America
C	Pacific Islands
D	South America
E	Future Use
F	Future Use

The following table is an example that has been created as a partial list of Minor Location for the "North America" Major Location of Earth. These assignments are suggestions and are not mandatory for use at this time.

Table 3: Minor Location Number Assignments for North America

Assignment	Minor Location
00	Alberta
01	British Columbia
02	Manitoba
03	New Brunswick
04	Newfoundland and Labrador
05	Northwest Territories
06	Nova Scotia
07	Nunavut
08	Ontario
08	Price Edward Island
0A	Quebec
0B	Saskatchewan
0C	Yukon
10	Hawaii
11	Alaska
12	California
13	Oregon
14	Washington

20	Arizona
21	New Mexico
22	Texas
23	Oklahoma
30	Nevada
31	Utah
32	Colorado
33	Wyoming
34	Idaho
35	Montana
40	North Dakota
41	South Dakota
42	Nebraska
43	Kansas
44	Minnesota
45	Iowa
46	Missouri
47	Wisconsin
48	Illinois
49	Michigan
4A	Indiana
4B	Ohio
50	Arkansas
51	Louisiana
52	Mississippi
53	Alabama
54	Georgia
55	Florida
56	South Carolina
57	North Carolina
58	Tennessee
59	Kentucky
5A	Virginia
5B	West Virginia
5C	Washington DC
60	Maryland
61	Delaware
62	New Jersey
63	Pennsylvania
64	New York
65	Connecticut
66	Rhode Island
67	Massachusetts
68	New Hampshire
69	Vermont
6A	Maine

70	Baja California
71	Baja California Sur
60	Sonara
61	Chihuahua
62	Sinaloa
63	Durango
70	Coahuila
71	Zacatecas
72	San Luis Potosi
73	Tamaulipas
74	Nuevo León
80	Nayarit
81	Jalisco
82	Colima
83	Aguascalientes
84	Guanajuato
90	Hildago
91	Querétaro
92	México
93	Mexico City
94	Morelos
95	Puebla
96	Tlaxcala
80	Veracruz
81	Tabasco
90	Michoacán
91	Guerrero
92	Oaxaca
93	Chiapas
A0	Campeche
A1	Yucatán
A2	Quintana Roo

The following table lists a small subset of recommended customer components for the “North America” major region’s “New York” minor region. These assignments are suggestions and are not mandatory for use at this time.

Table 4: Customer Component Number Assignments

Assignment	Customer Component
00	General Public
11	Hospital
12	Medical Services
13	Fire Services
14	Protective Services (police)
20	Judicial Government Services

21	Community Government Services (Libraries, social aid, etc.)
30	Military
40	Banks
50	Grocery Stores
60	Schools and Public Child Services
70	Telecommunications Service Provider

Assumptions

The assumptions that are known to exist when VEP was being developed include the following:

- Storage solutions will still ensure the integrity of data
- Storage solutions will only permit data read and write from the VEP Provider
- Network security will be used to prevent brute-force, DDOS, and other attacks
- Client devices will protect the identity specific private keys and/or certificates

VEP Components

There are three structural components to VEP which are described in this section. The VEP Provider facilitates the creation and use of VEP certificates and call management, the VEP client is a software package that is used by any entity that wishes to utilize the VEP protocol, and the VEP database is the storage solution which contains all available numbers, all numbers assigned to contacts, and all voice messages for each contact.

VEP Provider

The core component of the VEP infrastructure is the VEP Provider. The VEP Provider is responsible for, and facilitates, all VEP capabilities. There are four main areas of responsibilities that are placed within the charge of the VEP Provider which are certificate management, rotating VEP storage keys, and client authentication and authorization.

Certificate Management

There are three kinds of certificates which are managed by the VEP Provider, the VEP root certificate, the VEP Provider certificate, and the Client certificates. The VEP Provider certificate is used to create trust and non-repudiation between the VEP Provider and the client as well as encrypt global contents stored in the VEP Database. The VEP client certificates are used to create non-repudiation while facilitating confidentiality and integrity.

VEP Provider Certificate Management

When the VEP Provider is initially created a self-signed root certificate is created. This VEP root certificate is used to create all other certificates until it is replaced with a new VEP root certificate. At time of creation the VEP root certificate offer a one-time certificate export option for back-up and recovery purposes. After the VEP root certificate is created the first certificate created for use is VEP is the VEP Provider certificate. The VEP Provider certificate also offers a one-time certificate export option when it is created to facilitate back-up and recovery capabilities.

When a VEP root certificate requires replacement the best option is to decommission the VEP Provider and migrate all data and users to a new VEP Provider. This can be accomplished by creating a new VEP Provider, a VEP migration agent, and a new VEP database. The migration agent is granted ‘read’ access to all contents in the “old” VEP database and write access to all areas in the

"new" VEP database. All clients will be issued new certificates by the new VEP root certificate. Effectively, you will have two VEP databases with the same content with the original database having read-only access and the new database having read-write access. The new database is used Vfor all contact information and the old database get decommissioned through attrition. The process for rotating the VEP Provider certificate follows a similar set of steps.

Client Certificate Management

The VEP Provider is responsible for creating, maintaining, and authenticating client certificates. The VEP Provider syncs with the VEP specific groups in the enterprises user database daily by default with the option to sync hourly, every 6 hours, twice daily, or daily. When new users are discovered the VEP Provider provisions a client certificate for the user and adds contact details and a voice message space in the VEP database; likewise, when a user is removed from any VEP specific groups in the enterprise user database the associated certificate is revoked and the VEP database is updated. For the initial client certificate the VEP Provider takes an additional step of provisioning a VEP software package for the new user and emailing a one-time enrollment code to the new user.

VEP Client Integration

Clients that wish to use VEP must use the VEP software package to enroll. The software package facilitates the installation of the VEP root certificate, the retrieval and installation of the VEP client certificate, making voice calls, and managing voice messages. The VEP client software package is made available by the VEP Provider for download using a one-time user-specific code that was created by the VEP Provider and an organization specific code. The VEP user navigates to the VEP Provider web portal, enters the required information and codes, then downloads the prepared software package. Once the package is downloaded it creates a secure connection to the VEP Provider to download and install the VEP root certificate and client certificate after-which the client software deletes enrollment specific keys and codes.

Once the VEP Provider root certificate is installed in the trusted root store and the client certificate is enrolled in the user certificate store the VEP software creates a contacts database. The contacts database is a store of contacts with their public keys and associated data that is used to identify clients. The data used to identify clients include the client's username, the client's assigned phone number, and the client's organization. The client's phone number is the only piece of information that is not included in the certificate as this is the only piece of required information that is subject to change more frequently than the client's certificate.

VEP Blob Storage

VEP blob storage is a database that manages and stores VEP phone number assignments and voice messages. As such, VEP storage is segmented into two high level storage spaces, the "Contacts Storage Space" area and the "Voice Messages Storage Space".

Contacts Storage Space

The contacts storage space has two main components, the unassigned numbers space and the contact details space. The unassigned numbers space is segmented into phone number tables based on an organization defined prefix. The organization defined prefix may be the first one, two, or three digits of the "customer assignment" portion of the phone number structure. This permits the organization to use all 4,294,967,296 possible number at once or create up to 4,096 tables of 268,435,456 available

phone numbers. Organizations can segments various portions of the organization and use phone number assignment more efficiently through segmentation. When a number is assigned to a contact it is removed from an available phone number table that has been authorized for use. As part of the assignment process the assigned phone number is entered into the contact details space along with the client's public certificate. An additional position in the contacts details space is created for every contact, the voice message status code space. The voice message status code space is a non-VEP-encrypted management space that indicates if a voice message storage space has been created and if the user has provisioned the storage space to receive messages. The contact details storage space runs a job every 15 minutes to update the voice message status code. The codes for this space are as follows:

- 1 – storage space not created
- 2 – storage space created but not provisioned
- 3 – storage space created and user has provisioned

Voice Messages Storage Space

The voice messages storage space area of VEP storage runs a task every 15 minutes to scan the contacts storage space to find any "3" codes in the status space of the contact details. If any "3" codes are located a new space is created to store the voice messages of the associated contact. The space contains three parts:

1. The user identifier (the public certificate)
2. A "greeting" space used to store greetings for anyone wishing to leave a message
3. A "messages" space used to storage any messages that have been provided for the contacts

VEP Implementation and Use

Having a VEP infrastructure has little significance if there is no way to use VEP. The use of VEP is reliant on proper routing between VEP Providers (usually disparate organizations), the ability to create new contacts and update contact details, place VEP calls, and retrieve VEP messages.

VEP Routing

Not all VEP clients will be enrolled with the same VEP Provider; therefore, the ability for clients to reach clients that are enrolled with other VEP Providers is essential. VEP routing is hierarchical and follows the hierarchy of the VEP phone number structures in revers order. If a client wishes to place a call to another client that is not enrolled in the same VEP Provider the following steps are taken:

1. The VEP Provider determines if the intended recipient has the same "Space Site" in the phone number.
   a) If no, the VEP Provider sends an error message to the user "Sorry, we have not colonized space yet".
   b) If Yes, the VEP Provider proceeds to step 2.
2. The VEP Provider determines if the intended recipient has the same "Major Location" in the phone number.
   a) If no, the VEP Provider forwards the connection request to one of the five VEP Providers in the target location that are in its "Major Location" database. If the forward request fails to reach the chosen VEP Provider it retries the same VEP Provider two additional times before tying the remaining 4 VEP Providers 3 times each. If none of the five VEP Providers accept the connection request the caller receives the "call failed" error message.
   b) If Yes, the VEP Provider proceeds to step 3.

3. The VEP Provider determines if the intended recipient has the same “Minor Location” in the phone number.
    a) If no, the VEP Provider forwards the connection request to one of the three VEP Providers in the target location that are in its “Minor Location” database. If the forward request fails to reach the chosen VEP Provider it retries the same VEP Provider two additional times before tying the remaining 2 VEP Providers 3 times each. If none of the five VEP Providers accept the connection request the caller receives the “call failed” error message.
    b) If Yes, the VEP Provider proceeds to step 4.
4. The VEP Provider determines if the intended recipient has the same “Customer Component” in the phone number.
    a) f no, the VEP Provider forwards the connection request to one of the three VEP Providers in the target location that are in its “Customer Component” database. If the forward request fails to reach the chosen VEP Provider it retries the same VEP Provider two additional times before tying the remaining 2 VEP Providers 3 times each. If none of the five VEP Providers accept the connection request the caller receives the “call failed” error message.
    b) If yes, the caller receives an error message “Contact not found”.

Updating Contact Details

When a client or organization wishes to update the contact details of a user the update must be performed in a way that ensures confidentiality, non-repudiation, and authenticity; Therefore, there are only two ways to update a contact’s details: disable the contact or perform a contact initiated update.

Disabling a Contacts

When an organization wishes to remove a contact from the VEP Provider and VEP database the organization must remove the contact from the VEP specific group in the organization’s user database. Once the VEP Provider syncs with the organization’s user database the changes will take effect. The changes that occur are:

1. The VEP Provider places the user’s certificate in a “revoked stage 1” status with a timestamp. This stage permits the user to be reactivated and permit full restoration of the account within 7 days of the time and date of disablement.
2. After 7 days have passed from the time and date the user was disabled in the organization’s user account database the user’s certificate enters “revoked stage 2” status. In this status the VEP Provider removes all saved voice messages and contact details from the VEP database.
3. Thirty days after a user certificate enters “revoked stage 2” the phone number associated with the account is listed as available for assignment in the VEP database.

Contact Initiated Update

When a contacts wish to update their personal details or phone number they can user the client software package to update the database. The flows for a contact initiated update is as follows:

1. The user opens the client software and indicates an updated is requested
2. The user indicates the type of change the user would like to make: username or phone number
3. The user enters the desired username or phone number
4. The client software submits the request to the VEP Provider
5. The VEP Provider forwards the phone number and/or username to the VEP database to check for availability. If the requested change is available the change is submitted and confirmed with the user. If the requested change is in use by another user the VEP Provider proceeds to step 6.
6. The VEP Provider adds adds 5 pseudo-random characters to the username and/or requests 5 available phone numbers from the VEP database.

a) The VEP Provider confirms availability of the new username with the VEP database
b) If the new username is not available the VEP Provider adds an additional 5 pseudo-random characters to the username and checks for availability. If not available to VEP Provider sends a "username not available please try again" error to the user. If it is available the VEP Provider proceeds to step 7.

7. The VEP forwards the recommended username and/or available phone number to the user and asks the user to accept the username and/or choose a phone number.
   a) If the user confirms the selection the VEP Provider checks the availability again then assigns the new username and/or phone number in the database. For new usernames a new client certificate is issues.
   b) If the user rejects the recommended username or phone number the user returns to step 3.

Placing A Call

When a user wishes to place a call there are a number of steps that must occur to ensure security and privacy. All users have the ability to make their contact details available to other in the VEP contact store by choosing one of the following four settings.

1. Make my information available to everyone
2. Make my information available to my organization
3. Make my information available to users I call (default)
4. Make my information available to nobody

When a user wishes to place a call to a user that is stored in the local database instead of the VEP Contact store the VEP software package must verify the correct recipient details are being used, determining if the recipient is available (answers the call), and enable the ability to leave a voice message if the recipient is unavailable. When a user places a phone call to a recipient the client software performs the following steps:

1. Determines if the phone number is in the local contact databases
   a) if yes, the software uses the stored contact details
   b) if no, the software requests the contact details from the VEP contact store
      1. The VEP Provider checks the contact's privacy settings (the 4 listed above) and forwards the number or returns a denied message as appropriate.
2. Once the contact data is obtained the VEP Client creates a connection request which is encrypted using the recipient's public key and attaches header information indicating the required recipient data.
3. The encrypted request with headers is forwarded to the VEP Provider.
4. The VEP Provider verifies the phone number prefix matches the organization and is internal.
   a) If the number is not within the organization the VEP Provider uses VEP routing to forward the call
   b) If the number is within the organization the contact details are verified in the database.
5. If details match the information stored in the VEP database the call request is forwarded to the intended recipient otherwise the VEP Provider rejects the request.
6. Once the recipient receives the call it can be accepted or rejected.
   a) If accepted, a connection is made,
   b) If the recipient is not available the caller is permitted to record a voice message.
   c) If the recipient rejects the call the recipient can permit or deny the caller the ability to leave a voice message.

Verifying Recipient Details

When a VEP Provider receives a request to connect a caller to a recipient it must verify the caller is providing the correct recipient details. To do this the VEP Provider reads the certificate serial number, and phone number from the connection request header. This information is encrypted using the VEP Providers private key and forwarded to the VEP database. The VEP database searches its contact list to determine if it has a matching entry then forwards the result back to the VEP Provider. If the VEP database confirms a match the VEP Provider forwards the request to the recipient. If the VEP database does not have a matching entry the VEP Provider responds to the caller with a "user not found" error message.

If Recipient Is Available

Once the connection request reaches the recipient the recipient can choose to answer the call. When the recipient answers the call the following steps are taken:

1. The recipient's client software creates an "accept call" packet and encrypts it with the caller's recipient's private key, then the caller's public key, followed by the VEP Provider's public key.
2. The recipient's client software adds the caller's required information to the header (certificate serial number and phone number)
3. The "accept call" packet is forwarded to the VEP Provider.
4. The VEP Provider uses the VEP Provider private key to decrypt the message the encrypts the message with the caller's public key.
5. The VEP Provider forwards the "accept call" packet to the caller.
6. The caller uses the caller's private key twice followed by the recipients public key to remove the encryption.
7. The caller creates a "call accepted" packet and encrypts it with the caller's private key followed by the recipient's public key followed by the VEP Provider's public key.
8. The caller forwards the packet to the VEP Provider
9. The VEP Provider verifies the details and forwards the message to the recipient.
10. The connection is established until the VEP Provider receives an "end call" packet or the session times out after 30 seconds of no activity.

If Recipient Is Not Available

When the connection request reaches the recipient:

1. The recipient is forwarded 3 consecutive connection request from the VEP Provider
2. The VEP Provider retrieves the recipient's voice message greeting from the VEP database
3. The VEP Provider forwards the voice message greeting to the caller
4. The caller software records a voice message
5. The voice message is forwarded to the VEP Provider
6. The VEP Provider stores the voice message in the VEP database for the appropriate recipient

If Recipient Rejects The Call

The following flow is completed when a recipient chooses to reject an incoming call:

1. The recipient sees a prompt with the following three options:
   a) Answer Call (this option follows the steps in "Recipient is Available" above)
   b) Send to Voicemail (this option manually triggers step 2 of "If Recipient Is Not Available")
   c) Reject Call
2. If the recipient chooses to reject the call the following steps are taken:
   a) The recipient's software creates a "reject call" packet

b) The packet is encrypted with the recipients private, the caller's public key, then the VEP Provider's public key
c) The "reject call" packet is forwarded to the VEP Provider
d) The VEP Provider uses its private key to verifies the details of the packet
e) The VEP Provider encrypts the packet with the caller's public key
f) The VEP Provider forwards the packet to the caller
g) The caller uses its private key to decrypt the packet twice then the recipients public key to remove the final layer of encryption
h) The caller software presents the caller with a "call rejected" message and terminates the session

Retrieving Voice Messages

When a user wishes to retrieve their voice messages the following actions occur:

1. The user opens the VEP client software
2. The user selects the option to retrieve voice messages (which are retrieved every 30 seconds by default)
3. The client software creates a "retrieve messages" packet and encrypts it with the client's private key
4. The packet is forwarded to the VEP Provider
5. The VEP Provider use the certificate serial number and phone number combination in the header to retrieve the correct public key
6. The VEP Provider verifies the authenticity of the request by ensuring the requested messages belong to the same entity to which the certificate was assigned
7. The VEP Provider retrieves the voice messages from the VEP Database (which were encrypted using the recipient's public key followed by the VEP Provider's private key)
8. The VEP Provider removes the VEP Provider encryption and encrypts the messages with the recipient's public key.
9. The recipient software decrypts the voice messages twice using the recipients private key
10. The recipient software adds the voice messages to the local voice message database with the appropriate flags set
    a) a – new message
    b) b – read message
    c) c – delete from local messages
    d) d – delete from VEP database
    e) e – delete from VEP database and local messages
11. Once the messages have been loaded into the local message database with the appropriate flags set the recipient can listen to new messages and have the flag automatically changed to "b" or can manually select messages individually or in bulk and change the flag

Summary

Voice Encryption Protocol (VEP) is a conceptual technical protocol that has been designed to increase the security and privacy that users can expect when placing or receiving voice calls or voice messages. This is an early stage conceptual protocol and is open for adjustment, refinement, discussion, creation, or rejection. This conceptual protocol document is intended to be a fairly comprehensive guide to ideas that can help to modernize and advance the voice call technology currently employed. VEP uses an advance phone numbering standard to increase the number of available phone numbers and provide more transparency about callers while increasing privacy and reducing the attack surface. The core

infrastructure components of VEP are the VEP Provider, the VEP database, and the VEP client software package. The routing of VEP calls follows a very organized structure designed to reduce call failures and increase routing efficiency. The VEP protocol can be used to create and update contacts, place a call, and retrieve and manage voice messages and settings. Voice Encryption Protocol (VEP) is a conceptual technical protocol that offer a wide array of benefits that simply do not exists in current voice technology solutions.