

AFRL-IF-RS-TR-2005-96  
Final Technical Report  
March 2005



## VOLTAGE IDENTITY BASED ENCRYPTION (VIBE)

Voltage Security, Inc.

Sponsored by  
Defense Advanced Research Projects Agency  
DARPA Order No. S702

*APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.*

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the Defense Advanced Research Projects Agency or the U.S. Government.

AIR FORCE RESEARCH LABORATORY  
INFORMATION DIRECTORATE  
ROME RESEARCH SITE  
ROME, NEW YORK

## STINFO FINAL REPORT

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2005-96 has been reviewed and is approved for publication

APPROVED:                   /s/  
MELVIN J. OSTER  
Project Engineer

FOR THE DIRECTOR:                   /s/  
WARREN H. DEBANY, JR.  
Technical Advisor  
Information Grid Division  
Information Directorate

| REPORT DOCUMENTATION PAGE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                 |                                                                                              | Form Approved<br>OMB No. 074-0188    |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------|--------------------------------------|--|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                 |                                                                                              |                                      |  |
| 1. AGENCY USE ONLY (Leave blank)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2. REPORT DATE<br>March 2005                                    | 3. REPORT TYPE AND DATES COVERED<br>Final May 04 – Aug 04                                    |                                      |  |
| 4. TITLE AND SUBTITLE<br><br>VOLTAGE IDENTITY BASED ENCRYPTION (VIBE)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                 | 5. FUNDING NUMBERS<br>C - FA8750-04-C-0217<br>PE - 62301E<br>PR - S702<br>TA - VI<br>WU - BE |                                      |  |
| 6. AUTHOR(S)<br><br>Mark J. Schertler<br>Prashanth Koppula                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                 |                                                                                              |                                      |  |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br><br>Voltage Security, Inc.<br>1070 Arastradero Road<br>Palo Alto CA 94304                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                 | 8. PERFORMING ORGANIZATION<br>REPORT NUMBER<br><br>N/A                                       |                                      |  |
| 9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)<br><br>Defense Advanced Research Projects Agency<br>3701 North Fairfax Drive<br>Arlington VA 22203-1714                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                 | 10. SPONSORING / MONITORING<br>AGENCY REPORT NUMBER<br><br>AFRL-IF-RS-TR-2005-96             |                                      |  |
| 11. SUPPLEMENTARY NOTES<br>DARPA Program Manager: Tim Gibson/ATO/(703) 526-4764<br>AFRL Project Engineer: Melvin J. Oster/IFGA/(315) 330-1870<br>Melvin/Oster@rl.af.mil                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                 |                                                                                              |                                      |  |
| 12a. DISTRIBUTION / AVAILABILITY STATEMENT<br><br>APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                 |                                                                                              | 12b. DISTRIBUTION CODE               |  |
| 13. ABSTRACT (Maximum 200 Words)<br>Invented by Dr. Dan Boneh and Dr. Matt Franklin in 2001, Identity-Based Encryption, or IBE, is a breakthrough in cryptography that, for the first time, enables users to simply use an identity, such as an email address, to secure business communications. This replaces the digital certificates that a traditional X.509 based public key infrastructure (PKI) relies on. Moreover, unlike existing security solutions, secure communication based on IBE technology can be conducted online as well as offline, from anywhere in the world, without the complexity of certificates, Certificate Revocation Lists (CRLs) and other costly infrastructure. IBE is transparent to end users, easy to deploy and manage, and can scale to millions of users on the internet.<br><br>Contract FA8750-04-C-0217 was awarded to Voltage Security, Inc., to demonstrate the effectiveness of the technology developed to implement the Boneh-Franklin IBE. This contract provided for the necessary hardware and software needed to demonstrate the Voltage technology, as well as necessary supporting services needed to implement the technology. |                                                                 |                                                                                              |                                      |  |
| 14. SUBJECT TERMS<br>Cryptography, certificate, identity, secure communications, JWID                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                 |                                                                                              | 15. NUMBER OF PAGES<br>36            |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                 |                                                                                              | 16. PRICE CODE                       |  |
| 17. SECURITY CLASSIFICATION<br>OF REPORT<br><br>UNCLASSIFIED                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 18. SECURITY CLASSIFICATION<br>OF THIS PAGE<br><br>UNCLASSIFIED | 19. SECURITY CLASSIFICATION<br>OF ABSTRACT<br><br>UNCLASSIFIED                               | 20. LIMITATION OF ABSTRACT<br><br>UL |  |

## Table of Contents

|                                            |    |
|--------------------------------------------|----|
| Introduction.....                          | 1  |
| Identity-Based Encryption (IBE) .....      | 1  |
| Introduction to Voltage Security, Inc..... | 3  |
| SecureMail .....                           | 4  |
| Exercise Goals .....                       | 7  |
| JWID Executive Summary .....               | 8  |
| DP04 Executive Summary .....               | 10 |
| References.....                            | 12 |

## List of Appendixes

|                                                                                                                                                                                           |    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Appendix A Voltage Identity Based Encryption (VIBE) For the Creation of Dynamic Coalitions: A Demonstration of Capabilities at the 2004 Joint Warrior Interoperability Demonstration..... | 13 |
| Appendix B Voltage Identity Based Encryption (VIBE) For the Creation of Dynamic Coalitions: Demonstration of Capabilities at the Determined Promise 2004 (DP04) Exercise.....             | 23 |

## List of Figures and Tables

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| Figure 1: How IBE works.....                                            | 2  |
| Figure 2: Secure Mail features.....                                     | 5  |
| Figure 3: SecureMail Example .....                                      | 6  |
| Figure 4: Network architecture for VIBE deployment at JWID 04.....      | 17 |
| Figure 5: Network connectivity for the VIBE trials at JWID 04.....      | 18 |
| Figure 6: Network architecture for VIBE deployment at DP04. ....        | 28 |
| Figure 7: Network connectivity for the VIBE deployment at DP04. ....    | 29 |
| Table 1: MSEL events exercising VIBE technology in trial UST 01.09..... | 20 |

# Introduction

Invented by Dr. Dan Boneh and Dr. Matt Franklin in 2001, Identity-Based Encryption or IBE, is a breakthrough in cryptography that, for the first time, enables users to simply use an identity, such as an email address, to secure business communication. This replaces the digital certificates that a traditional X.509 based public key infrastructure (PKI) relies on. Moreover, unlike existing security solutions, secure communication based on IBE technology can be conducted online as well as offline, from anywhere in the world, without the complexity of certificates, Certificate Revocation Lists (CRLs) and other costly infrastructure. IBE is transparent to end users, easy to deploy and manage, and can scale to millions of users on the internet.

The initial research that led to the development of a practical Identity Based Encryption technology was funded by DARPA contract F30602-99-1-0530. This project led to the invention of Boneh-Franklin IBE [1], the first IBE technology that was found to be both feasible to implement as well as secure.

An additional contract, contract FA8750-04-C-0217, was awarded to Voltage Security, Inc., to demonstrate the effectiveness of the technology developed to implement the Boneh-Franklin IBE. This contract provided for the necessary hardware and software needed to demonstrate the Voltage technology, as well as necessary supporting services needed to implement the technology.

The first phase of the demonstration of the Voltage IBE (VIBE) technology took place at the 2004 Joint Warrior Interoperability Demonstration (JWID 04). At JWID 04, Voltage technology was installed and used at five different sites, and proved to easily allow secure communication between the sites, both through e-mail and through messages sent to BlackBerry handheld devices.

The second phase of the demonstration of the Voltage IBE (VIBE) technology took place at the 2004 Determined Promise (DP04) exercise. At DP04, Voltage technology was installed at USNORTHCOM, at Peterson Air Force Base, with the intent of using it to provide easy-to-use secure communication with several sites throughout the states of California and Virginia.

## *Identity-Based Encryption (IBE)*

IBE involves the encryption of data using an IBE public key. The encrypted data can later be decrypted using an appropriate private key. The IBE public key does not need to be known or established prior to the encryption process, and can be any arbitrary string, such as an email address. This significantly reduces the requirements for infrastructure in an IBE system and allows the public key itself to specify policy. A person can receive a secure signed and encrypted email without being enrolled in the system; the first secure

email walks the receiver through the process of registration and acquiring decryption keys. Thus secure communities of interest can be established for communication on the fly.

An IBE public key can specify user identification, expiration period, group membership and many other policy attributes. These attributes can all be verified during private key generation so that security policy may be centrally controlled. When set to a short time period, the expiration date facilitates removing a person from the system quickly. Rather than using a Certificate Revocation List (CRL) where a list of expired or revoked certificates is transmitted to everyone in the system, IBE allows the administrator to simply remove the person's ability to decrypt messages by quickly expiring an individual's decryption keys.

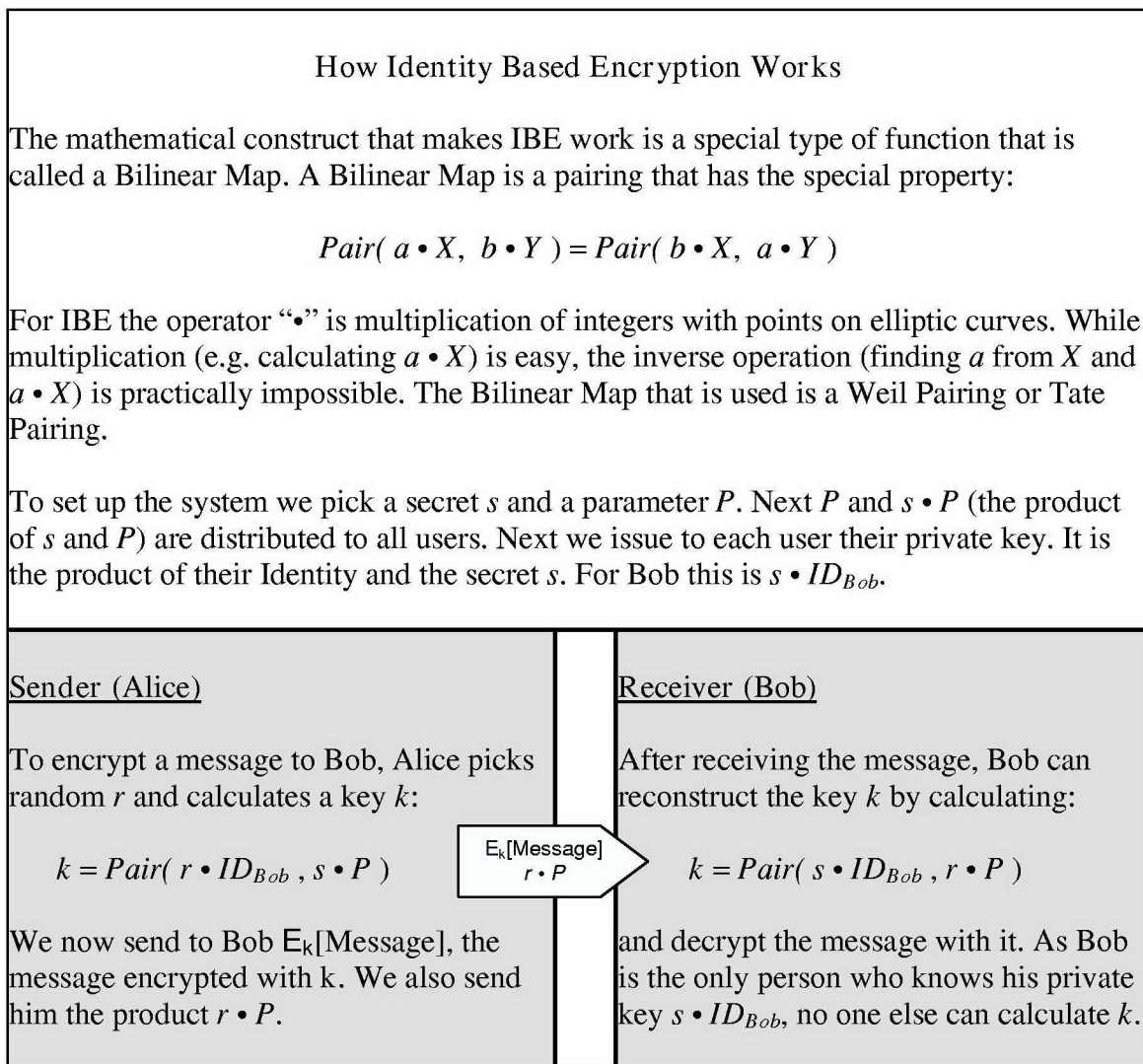


Figure 1: How IBE works

Traditional X.509 based PKI suffers from several shortcomings, including the difficulty of distributing and using digital certificates, the lack of PKI-enabled applications, and an extremely high total cost of ownership. It is possible to use IBE technology instead of X.509 based PKI to provide the same benefits to users (confidentiality and integrity of information, etc.), but at a greatly reduced cost. The practical application of IBE results in a solution that is easy to implement and easy to manage, without the overhead and cost inherent in traditional security solutions. The scalability of the IBE approach means that, for the first time, enterprises can communicate securely with their clients opening up new business opportunities, better customer service and, most importantly, differentiated competitive advantage.

### *Introduction to Voltage Security, Inc.*

Voltage Security, Inc. is an information security company that was founded in 2002 to develop a security platform providing secure multi-channel business communication solutions for the enterprise market based on IBE technology. Voltage is the first to use identity to bring confidence to business communication. Voltage solutions secure business communication by making anytime, anywhere communication easy to use and painless to deploy.

The Voltage Security Platform built on IBE technology, removes the hurdles associated with public key infrastructure, and is composed of several products:

- Voltage SecurePolicy Suite – A central enterprise security server used to enforce security policies related to the issuance of IBE keys, user provisioning, and administration of mission critical business communication.
- Voltage SecurePolicy Service – A managed service for the Voltage SecurePolicy Suite and applications, available today for pilot applications.
- Voltage SecureMail – A software agent used with existing email solutions to enable users to transparently send and receive secure email.
- Voltage SecureMail for Blackberry – A Blackberry Enterprise Server (BES) plugin that allow SecureMail messages to be decrypted and read on Blackberry devices.
- Voltage SecureFile – A software agent to enable users to transparently secure files, directories and documents on portals and intranets.
- Voltage SecureChat – A client / server application that provide the ability for groups to securely establish and communicate via a shared communication (chat) channel.
- Voltage Enrollment Server – A web-based application that supports the ability to create and manage ad hoc groups. The Enrollment Server operates in conjunction with the Voltage Secure Policy Suite to provide a flexible and manageable method for provisioning users and groups.

Voltage enterprise solutions are broadly applicable to any organization with information security and compliance requirements such as those found in financial services, government, healthcare and insurance.

## *SecureMail*

Voltage SecureMail is a software module that works with various existing email applications and enables users to send email, including attachments, securely anytime, anywhere, and transparently. Identity-Based encryption protects the email by encrypting it to all authorized recipients. Digital signatures are used to authenticate the origin and content of an email message. Voltage SecureMail leverages S/MIME with IBE for the key exchange, allowing users to encrypt messages without knowing anything beyond the recipient's email address. Voltage SecureMail is the first secure email solution that makes secure, ad hoc business communication as easy as traditional, non-encrypted messaging.

The Voltage SecureMail client integrates seamlessly into existing email applications. All that is required to send a secure signed and encrypted message is the identity (email address) of the person receiving the message. Therefore, how a person interacts with their existing application is unchanged; the sender and receiver do not have to know anything about the underlying infrastructure or technology to communicate securely.

Voltage SecureMail enables users to:

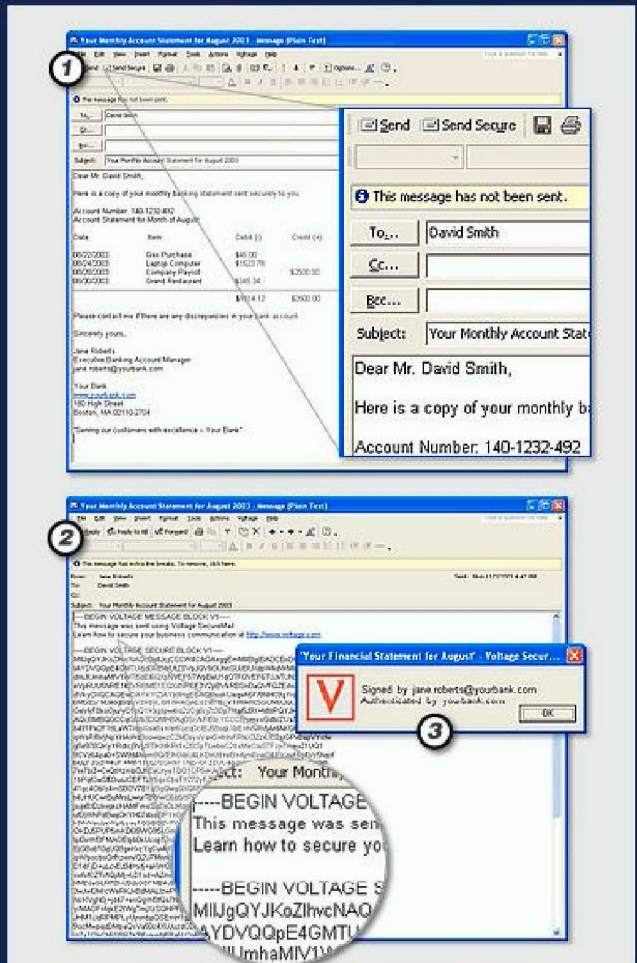
- Send secure messages to the extended enterprise, without pre-enrolling recipients
- Transparently send secure emails using existing mail systems, without learning new techniques
- Encrypt and decrypt messages online and offline, and view them anywhere on the internet through transparent roaming
- Send emails with the confidence that they can be read by recipients regardless of email system
- Deliver messages using the Voltage Zero Download Reader (ZDR), which does not require the recipient to install or download any software

Corporations can use Voltage SecureMail to ensure that key business processes are compliant with regulations such as Sarbanes-Oxley and the Gramm-Leach-Bliley Act. They can also, for the first time, securely communicate with their customers via email, without the need for complex setup or change of behavior on the customer side. These benefits open up a number of business opportunities not possible with existing solutions; for example, treasury operations can now be conducted securely via email in a natural ad-hoc fashion.

Voltage SecureMail enables users to send secure, ad hoc business communication such as financial statements, patient health information (PHI) or sensitive communication regarding intellectual property. Such critical communication is conducted in a transparent and flexible way without demanding complex end user training and administration. No pre-enrollment of recipients is required. And, because Voltage SecureMail uses existing user identities, such as email addresses, as encryption keys, no extra steps or clicks are required.



Figure 2 below shows the various feature of SecureMail via an example.



The figure consists of two screenshots of an email client interface. The top screenshot shows an email being composed. A red circle with the number '1' highlights the 'Send Secure' button in the toolbar. The email content is a 'Your Monthly Account Statement for August 2003'. The bottom screenshot shows an email that has been received and is encrypted. A red circle with the number '2' highlights the encrypted body of the email. A third red circle with the number '3' highlights a digital signature block at the bottom of the email, which includes a signature icon and the text 'Signed by jane.roberts@yourbank.com'.

**1 'Send Secure' Button**

Sending secure email is easy - just compose your message, add the recipient and press the send secure button on your email client. The email will be encrypted and sent to the recipient with a digital signature incorporated.

**2 Received Encrypted Message**

The first time an encrypted message is received, you will see an email consisting of a header and cipher text. The header contains instructions for where to go to download the Voltage SecureMail agent and to get a key. Just click on the link to start the process. Once the agent is installed, all messages will automatically be decrypted as you click on them.

**3 Digital Signature**

To protect against spoofing and to verify the sender, each message sent using Voltage SecureMail incorporates a digital signature that identifies the sender of the email. Any message with an invalid signature is automatically flagged.

Figure 2: Secure Mail features

#### Features of Voltage SecureMail:

- Integrates with existing email infrastructure – No need to deploy complex infrastructure. Easy and inexpensive to deploy.
- Transparent integrates with standard email clients – Easy to use. No training and education needed for users.
- Secure ad hoc business communication – Anyone can receive secure email even if not previously registered.
- 100% Comprehensive Coverage – Recipients can decrypt mail by using the Voltage SecureMail agent, which integrates directly into their email client, or by using the Voltage Zero Download Reader which requires no software to decrypt.
- Encryption based on group policy – Complete flexibility in creation of secure policies. Central access control.

- Offline usage and transparent roaming – Able to create and view secure email anytime, anywhere.

The following example (Figure 3) illustrates how Voltage SecureMail based on VIBE technology can be used to communicate securely. Alice at Company A would like to send her customer, Bob at Company B, a sensitive email that must be secure for compliance reasons. She uses Voltage SecureMail to send the secure email to Bob.

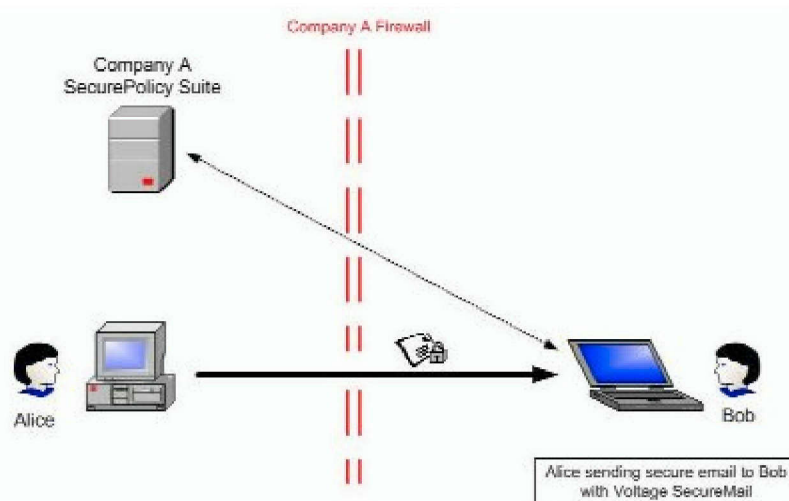


Figure 3: SecureMail Example

After Alice composes the email, she simply hits the Send Secure button, which automatically secures the email, along with any attachments, using Bob's email address "bob@b.com". Voltage SecureMail does not require pre-enrollment of users to receive secure email; even if Bob has never previously communicated with Alice or has never used Voltage SecureMail, he is still able to receive secure email from Alice.

The first time Bob receives the secure email on his laptop, Bob clicks on a link in the message header and downloads the Voltage SecureMail client. He then proceeds to enroll and authenticate to Company A's SecurePolicy Suite. The method used to authenticate Bob is completely flexible to the requirements of the enterprise.

Upon completion of proper authentication, the SecurePolicy Suite will present Bob with his private key to read the sensitive email. Alice and Bob can now communicate securely with Voltage SecureMail.

With his private key downloaded to his laptop, Bob can decrypt and view his received secure email even when he is offline on an airplane. Bob can even read his secure email at a business center using Voltage SecureMail's transparent roaming capabilities. In the case where Bob is reading his email using a client not currently supported by Voltage SecureMail, he can use Voltage SecureReader to view his secure messages.

The Voltage SecureReader attachment is available on all messages secured by Voltage SecureMail.

The Zero Download Reader (ZDR) functionality allows end-users who do not have an email client supported by Voltage to read, but not send, IBE-encrypted emails. If specified by the sender, the client plugin adds an HTML attachment to a Voltage SecureMail. If an e-mail recipient receives an IBE protected e-mail with the ZDR attachment but does not have a Voltage SecureMail agent installed, they can click on the ZDR attachment to view the message.

When the ZDR attachment is opened, and upon successful authentication to the ZDR server functionality at the VSPS, the ZDR attachment will be posted to the VSPS server for decryption and then displayed to the end user in a web browser. All ZDR communication is protected with the SSL protocol. Thus, the Voltage Zero Download Reader ensures that recipients can read encrypted mail messages anywhere, even if they do not have access to a supported mail application such as Outlook.

Additionally, SecureMail support also exists for BlackBerry as a fully-integrated security add-on to the BlackBerry Enterprise Server that provides easy-to-use, certificate-free content security for end-to-end Internet-based email transmission. This provides mobile professionals a secure and transparent way to protect the privacy of their communications at all times with customers, vendors and partners while ensuring compliance with federal privacy regulations. Voltage SecureMail BlackBerry allows BlackBerry users to use Voltage SecureMail to receive the plaintext (decrypted) version of Voltage-encrypted messages on their handheld device, encrypt messages from their handheld device, and reply to encrypted messages.

## *Exercise Goals*

USNORTHCOM's mission requires it to rapidly establish electronic communications with Federal, state, local, and private agencies and organizations as part of its response to crisis situations. Some of the information that must be exchanged in such situations is at the SBU/LES/FOUO level. Such information is readily exchanged with other DoD and Federal agencies that have approved secure communication capabilities employing hardware-based encryption. Until VIBE technology was invented, no means existed for exchanging of such information with organizations that did not have such equipment.

VIBE technology provides a potential means by which USNORTHCOM could exchange SBU/LES/FOUO information with organizations that do not possess hardware crypto. The JWID 04 and DP04 assessment were intended to determine if this technology provided the needed functionality, was acceptably easy to install and employ, and also to pilot a draft concept of operations for its use.

The overall goal of the effort was to assess the utility of IBE to provide for the exchange of encrypted emails within an operational community of interest (such as

USNORTHCOM and external agencies responding to a natural disaster or terrorist threat). Additional goals included validating a draft concept of operations for IBE and gauging ease of use.

The assessment also tried to determine VIBE's ability to provide the required functionality for operational use, and whether it can be installed, administered, and employed with acceptable effort by all participants.

Specific functionality that was exercised included:

- Provision of private keys to end user after authentication
- End users sending encrypted emails/attachments
- End users receiving and decrypting emails/attachments
- End users receiving and decrypting emails on BlackBerry devices
- Users who are not authenticated (do not have a currently valid private key) cannot decrypt encrypted emails
- Users read email using Zero Download Reader (ZDR)
- Instantiation of new users

## *JWID Executive Summary*

The 2004 Joint Warrior Interoperability Demonstration (JWID 04) provided a showcase for new technologies that have the potential to significantly assist elements of the US Department of Defense in accomplishing their missions.

VIBE technology was sponsored by DARPA for participation in JWID 04, and was designated US Trial 01.09. VIBE (UST 1.09) also partnered with US Trial 02.08 (New England Regional Threat Analysis Cell (NE-RTAC)). The JWID 04 exercise provides an opportunity for interested state and federal agencies to evaluate potentially interesting technologies in an environment that consists of a scripted exercise in which state and federal agencies simulate reacting to a variety of simulated disasters.

At JWID 04, Voltage technology was installed and used at five different sites, and proved to easily allow secure communication between the sites, both through e-mail and through messages sent to BlackBerry handheld devices. By sponsoring the use of VIBE technology in JWID 04, DARPA hoped to validate the use of VIBE technology as a potential supplement for traditional X.509 based PKI in next-generation secure systems.

After the VIBE software was installed and configured, role players in JWID 04 were able to communicate securely, both using e-mail from Microsoft Outlook and short text messages to and from BlackBerry handheld devices. Use of the Zero Download Reader (ZDR) option at one of the JWID sites also validated the capability of the VIBE technology to provide a secure communications channel without the need to install any client software at all.

Voltage Security, Inc. provided the following technologies for demonstration in JWID04:

- Voltage SecurePolicy Suite (VSPS)
- Voltage Chat Gateway
- SecureMail
- SecureFile
- SecureChat
- SecureMail for Blackberry (Blackberry Enterprise Server (BES) plug-in)
- Zero Download Reader.

The UST 01.09 trial installed server components at Peterson Air Force Base in Colorado Springs, Colorado and deployed client software at:

- Peterson Air Force Base
- Hanscom Air Force Base in Massachusetts
- SPAWAR naval facility in San Diego, California;
- DISA Eagle facility in Virginia
- Dahlgren Naval Surface Warfare Center in Virginia.

The execution phase of the UST 01.09 trial consisted of a total of 18 role players, representing the US Navy, US Coast Guard, and various staff elements of USNORTHCOM, who exchanged VIBE encrypted messages, both to and from Microsoft Outlook as well as to and from BlackBerry handheld devices. In each of these cases, all of the clients were required to install VIBE client software.

The UST 02.08 trial at Hanscom Air Force Base utilized the VIBE Zero Download Reader functionality. The VIBE SecureMail client was used to send secure messages via Outlook during UST 2.08. These secure messages were received by the federal, state, and local agencies participating in UST 2.08 and read using the Voltage Zero Download Reader. The Zero Download Reader allows users who receive Voltage SecureMail to view the messages in a web browser, which eliminates the need to install a SecureMail client on the users system.

The execution phase of the UST 02.08 trial consisted of one role player using Microsoft Outlook with the VIBE plug-in installed to communicate securely to other role players who had absolutely no additional client software installed. These additional role players represented the:

- US Army
- Massachusetts National Guard
- Massachusetts State Police
- State of Massachusetts,
- US Department of Justice
- Federal Emergency Management Agency.

Throughout the JWID 04 exercise, the use of VIBE technology was validated through the successful execution of events in the Master Scenario Event List (MSEL). MSEL events defined the use of the VIBE technology, and were designed to give several different

participants in JWID 04 a chance to test the VIBE technology. The key goal of JWID 04 was validating the capability of VIBE technology to quickly and easily create a dynamic coalition that could communicate securely, but without the usual overhead and burden associated with using encrypted communications.

Discussions with the JWID 04 participants before, during, and after the execution phase of the exercise validated that the VIBE technology was extremely easy to use, and provided a way to quickly deploy technology that allowed secure communications, but without the overhead involved with traditional PKI-based solutions. The use of VIBE technology allowed the efficient and rapid deployment of S/MIME security, but without the high costs associated with a full public key infrastructure.

A survey was conducted by UST 02.08 among the participants following the conclusion of the JWID 04 exercise. The responses to the survey questions [2] concerning VIBE technology were overwhelmingly positive. VIBE technology was characterized as a very valuable and a must have tool, one that demonstrated the most benefit to the end user. Feedback along similar lines was also received from UST 1.09 participants.

The JWID 04 exercise provided the opportunity for a number state and federal agencies to test the capabilities of the VIBE technology through a scripted exercise that tested the capabilities of VIBE enabled clients to communicate securely with both VIBE enabled clients as well as clients with no additional software installed. The technology proved simple and easy to use.

### *DP04 Executive Summary*

Determined Promise 2004 (DP04) was a North American Aerospace Defense Command and U.S. Northern Command (USNORTHCOM) homeland defense exercise which ran from August 5-10, 2004. This exercise tested USNORTHCOM's ability to assist civil and federal authorities in a coordinated response to simulated chemical, radiological, and explosive hazards, and was conducted in the states of California and Virginia.

VIBE technology was sponsored by DARPA for participation in DP04 to demonstrate the unique capabilities of the Voltage products to quickly and easily create dynamic coalitions of users, including elements of USNORTHCOM, the exercise leader, as well as the representatives of the States of California and Virginia, and FEMA Region III and Region IX. The key goal of DP04 was validating the capability of VIBE technology to quickly and easily create a dynamic coalition that could communicate securely, but without the usual overhead and burden associated with using encrypted communications. By sponsoring the use of VIBE technology in DP04, DARPA hoped to validate the use of VIBE technology to potentially supplement the X.509 based DoD PKI by providing a secure communications mechanism between the DoD and external agencies that are not on DoD PKI.



The VIBE software was installed and configured to allow the DP04 participants to communicate securely by using e-mail from Microsoft Outlook. Additionally, the Zero Download Reader (ZDR) option was turned on to allow secure communication channels between participants external to USNORTHCOM without the need to install any client software at all.

Voltage Security, Inc. provided the following technologies for demonstration at DP04:

- Voltage SecurePolicy Suite (VSPS)
- Voltage Enrollment Server
- SecureMail
- SecureFile
- Zero Download Reader (ZDR)

DP04 started on August 5<sup>th</sup> and ran through the 10<sup>th</sup>. The VIBE server software was successfully deployed at USNORTHCOM to support DP04 usage and fully functional as of August 4<sup>th</sup>. The VIBE technology was tested for readiness the day before the start of the DP04 exercises by personnel from both USNORTHCOM JCSC and Voltage Security to ensure that DP04 participants would be able to communicate securely with each other. The SecureMail client was downloaded by both an internal user and a user from Voltage acting as an external participant to verify that the software was correctly set up and that the exercise participants could communicate securely using VIBE technology.

USNORTHCOM maintains strict configuration control over user workstations and exercise participants did not have necessary permissions to download and install software. As a result, members of USNORTHCOM's Joint Communications Support Center (JCSC) were tasked with installing the VIBE SecureMail client software on each participating exercise workstation.

The Voltage personnel provided the USNORTHCOM JCSC personnel with client CDs and instructions on how to install the SecureMail client on the workstations of internal participants. Additionally, the USNORTHCOM JCSC personnel were also given instructions for the external participants to download the SecureMail client from the client download page hosted on the VIBE server in the DMZ.

Communication with the USNORTHCOM personnel during the DP04 exercise was severely limited. As of the end of the exercise on the 10<sup>th</sup>, no confirmation could be obtained from the USNORTHCOM J6 as to how many SecureMail clients were installed and how much usage the VIBE technology received.

The assessment fell short of what was originally intended. Due to circumstances that were beyond everyone's control the client software installation never took place, preventing exercise participants from using VIBE to encrypt and decrypt messages during the execution of the exercise scenario. The USNORTHCOM Server Room experienced flooding during the DP04 exercises as a result of flash flooding in Colorado Springs. This did delay the roll out of the SecureMail clients and perhaps the usage of VIBE at DP04.

Even though the assessment of the VIBE software during DP04 fell short of what was originally intended, the positive feedback from the UD04 and the JWID04 exercises has shown that the VIBE technology is a viable solution for supporting secure communications between diverse communities of interest where common authentication methods, such as PKI, are not shared.

## *References*

[1] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In Proc. Crypto '01, LNCS 2139, pages 213–229, 2001.

[2] Lt Col Donna L. Warner, USAFR. After Action Report JWID 2004 Regional Threat Analysis Cell (RTAC) US Trial 02.08 “Interagency Information Sharing”



Appendix A  
Voltage Identity Based Encryption (VIBE)  
For the Creation of Dynamic Coalitions:  
A Demonstration of Capabilities at the  
2004 Joint Warrior Interoperability  
Demonstration

## *Abstract*

The initial research that led to the development of a practical Identity Based Encryption (IBE) technology was funded by DARPA contract F30602-99-1-0530. This project led to the invention of Boneh-Franklin IBE [1], the first IBE technology that was found to be both feasible to implement as well as secure. This breakthrough in security technology allows the creation of secure communication channels, but without the burden and overhead associated with traditional public key infrastructure. It accomplishes this by using a user's e-mail address as their public key, thus avoiding the traditional problems with public key certification and distribution.

An additional contract, contract FA8750-04-C-0217, was awarded to Voltage Security, Inc., to demonstrate the effectiveness of the technology developed to implement the Boneh-Franklin IBE. This contract provided for the necessary hardware and software needed to demonstrate the Voltage technology, as well as necessary supporting services needed to implement the technology.

The first phase of the demonstration of the Voltage IBE technology took place at the 2004 Joint Warrior Interoperability Demonstration, JWID 04. At JWID 04, Voltage technology was installed and used at five different sites, and proved to easily allow secure communication between the sites, both through e-mail and through messages sent to BlackBerry handheld devices.

## *Summary*

The Voltage Identity Based Encryption (VIBE) technology developed by Voltage Security, Inc., was deployed to five different sites for use in the JWID 04 exercise. This technology comprised the necessary server software to implement VIBE as well as the client software needed for users to communicate securely.

The server software comprised the:

- Voltage Secure Policy Suite, the software product that securely generates and manages the cryptographic keys of the VIBE system
- BlackBerry Enterprise Server (BES) provided by Research in Motion (RIM);
- The Voltage Secure Blackberry plug-in to the BES to allow it to use VIBE to encrypt messages.

The client software comprised the Voltage SecureMail plug-in to Microsoft Outlook that allows a user to both encrypt and decrypt messages using VIBE technology.

Use of an additional server product, the VIBE SecureChat server, a product that allows the use of VIBE technology to secure IRC-style collaboration, but due to conflicts with the ports and protocols approved by DISA, the use of the SecureChat was not permitted, although the SecureChat server software was installed and tested.

After the VIBE software was installed and configured, role players in JWID 04 were able to communicate securely, both using e-mail from Microsoft Outlook and short text messages to and from BlackBerry handheld devices. Use of the Zero Download Reader (ZDR) option at one of the JWID sites also validated the capability of the VIBE technology to provide a secure communications channel without the need to install any client software at all.

## *Introduction*

VIBE technology is a breakthrough in encryption technology that allows a user to use his e-mail address as a public key, replacing the digital certificates that a traditional X.509 based public key infrastructure (PKI) relies on. Traditional PKI suffers from several shortcomings, including the difficulty of distributing and using digital certificates, the lack of PKI-enabled applications, and an extremely high total cost of ownership. By replacing X.509 based PKI with VIBE technology it is possible to provide the same benefits to users (confidentiality and integrity of information, etc.), but a greatly reduced cost. By sponsoring the use of VIBE technology in JWID 04, DARPA hoped to validate the use of VIBE technology as a potential replacement for traditional X.509 based PKI in next-generation secure systems.

The 2004 Joint Warrior Interoperability Demonstration (JWID 04) provides a showcase for new technologies that have the potential to significantly assist elements of the US Department of Defense in accomplishing their missions. VIBE technology was sponsored by DARPA for participation in JWID 04, and was designated US Trial 01.09. VIBE (UST 1.09) also partnered with US Trial 02.08 (New England Regional Threat Analysis Cell (NE-RTAC)). The JWID 04 exercise provides an opportunity for interested state and federal agencies to evaluate potentially interesting technologies in an environment that consists of a scripted exercise in which state and federal agencies simulate reacting to a variety of simulated disasters.

Voltage Security, Inc. provided the following technologies for demonstration in JWID04:

- Voltage SecurePolicy Suite (VSPS)
- Voltage Chat Gateway
- SecureMail
- SecureFile
- SecureChat
- SecureMail for Blackberry (Blackberry Enterprise Server (BES) plug-in)
- Zero Download Reader.

The UST 01.09 trial installed server components at Peterson Air Force Base in Colorado Springs, Colorado and deployed client software at:

- Peterson Air Force Base
- Hanscom Air Force Base in Massachusetts
- SPAWAR naval facility in San Diego, California;
- DISA Eagle facility in Virginia
- Dahlgren Naval Surface Warfare Center in Virginia.

The UST 02.08 trial at Hanscom Air Force Base utilized the VIBE Zero Download Reader functionality. UST 2.08 issued SITREPS and SPOTREPS securely via Outlook using the VIBE SecureMail agent. The secure messages were received by the federal, state, and local agencies participating in UST 2.08 and read using the Voltage Zero Download Reader. The Zero Download Reader allows users who receive Voltage SecureMail to view the messages in a web browser, which eliminates the need to install a SecureMail client on the users system.

Throughout the JWID 04 exercise, the use of VIBE technology was validated through the successful execution of events in the Master Scenario Event List (MSEL). MSEL events defined the use of the VIBE technology, and were designed to give several different participants in JWID 04 a chance to test the VIBE technology. The key goal of JWID 04 was validating the capability of VIBE technology to quickly and easily create a dynamic coalition that could communicate securely, but without the usual overhead and burden associated with using encrypted communications.

### *Methods, Assumptions, and Procedures*

Starting in March, 2004, the planning process for the use of VIBE software to provide secure communications between role players participating in the JWID 04 exercise began. Personnel from Voltage Security met with representatives of JWID 04 and the hosting command, USNORTHCOM, to discuss architectures for implementing the VIBE technology at JWID 04. The output of these meetings was an architecture that included two Voltage Secure Policy Suite (VSPS) servers installed at USNORTHCOM, two additional VSPS servers installed at a remote site (SPAWAR in San Diego, California) for backup and redundancy; one Voltage SecureChat server installed at USNORTHCOM; one BlackBerry Enterprise Server (BES) installed on the JWID 04 MACA network; and a VIBE plug-in to the BES that was also to be installed on the MACA network. The architecture that was agreed upon at these meetings is shown below in Figure 4. The full network connectivity for the VIBE trials is shown below in Figure 5.

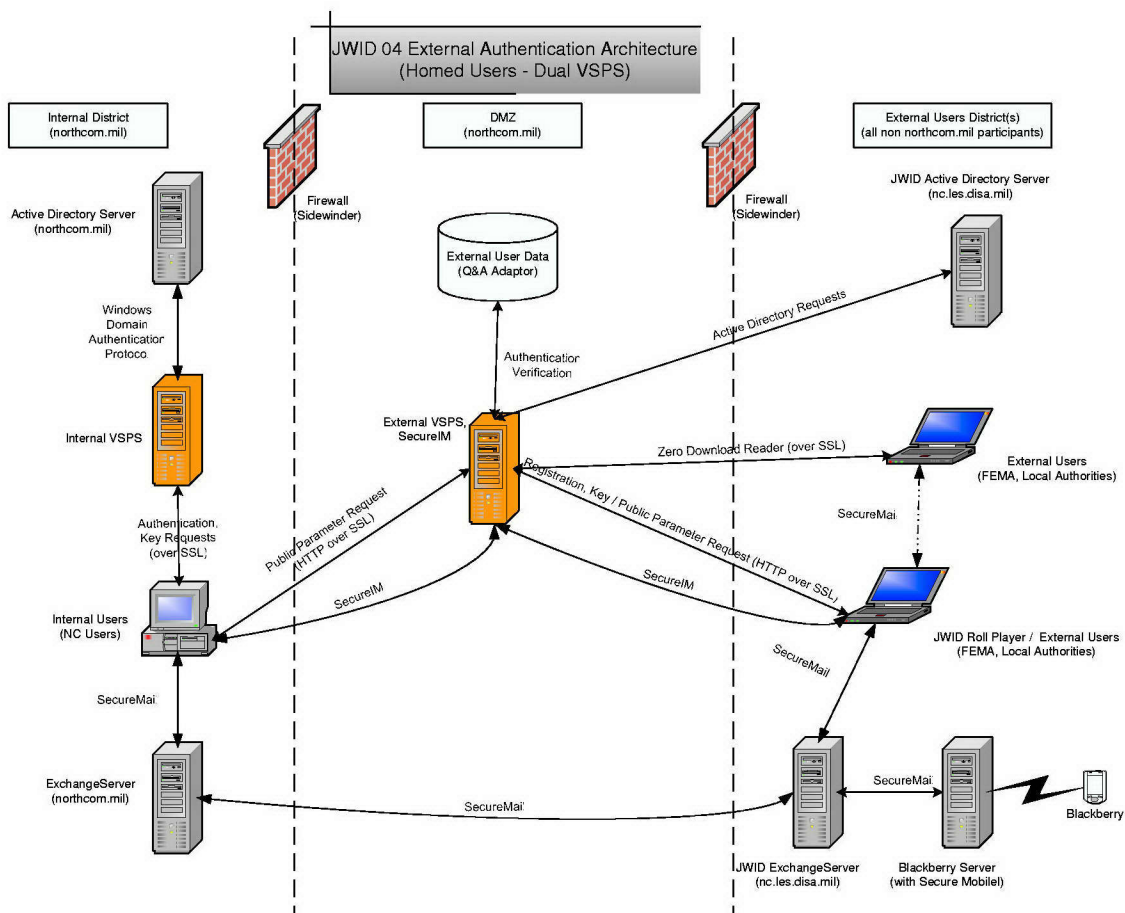


Figure 4: Network architecture for VIBE deployment at JWID 04.

## Internet Connectivity for Trials

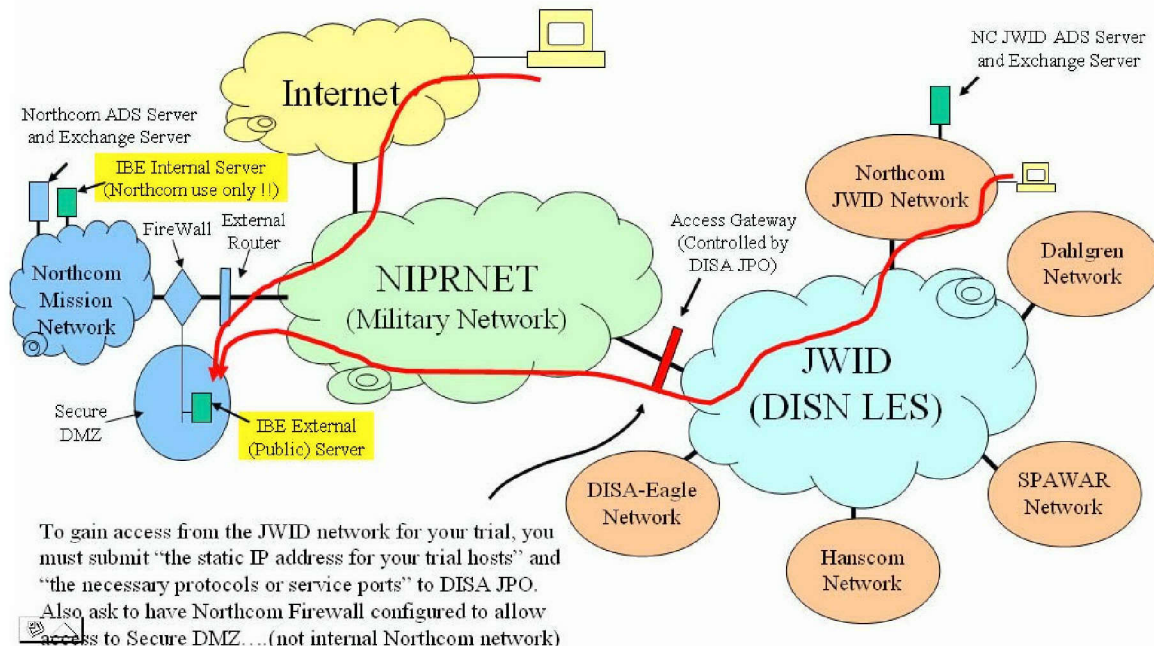


Figure 5: Network connectivity for the VIBE trials at JWID 04.

At this time, a detailed list of network configurations required for the operation of the VIBE products was provided to JWID 04 personnel. This list included the IP addresses required, as well as the ports and protocols necessary for the operation of the VIBE products.

After the completion of the JWID 04 planning meetings, continuous coordination between Voltage personnel and JWID 04 personnel ensured that the necessary hardware and software required for the implementation at JWID 04 was delivered as required, and that printed documentation on Voltage VIBE technology was available to JWID 04 participants and visitors during the exercise execution.

In addition, during the coordination period, extensive testing was performed by Voltage Security, Inc. engineers to ensure that the capabilities to be tested in JWID 04 would meet the usability needs of the JWID 04 role players. Product configuration refinements were completed during this period, and extensive work to make the user interface as easy to use as possible without compromising security was performed. Detailed step-by-step Task Guides that provided JWID 04 role players with accurate instructions on the operation of the VIBE technology were also prepared during this period.

The week of June 1, 2004 Voltage personnel traveled to Peterson Air Force Base to participate in JWID 04 set-up activities. During this week they installed and configured the VIBE servers at USNORTHCOM, and it was at the very end (Friday) of the set-up week that they were informed that the use of the VIBE SecureChat product was disallowed for JWID 04 due to conflicts with the list of approved ports and protocols maintained by DISA.

With the SecureChat product unavailable for use during JWID 04, Voltage personnel quickly adapted the MSEL events that were planned to use the SecureChat product into ones that used VIBE protected e-mail to accomplish the same collaboration as was planned for with the SecureChat.

During the week of June 1, 2004, Voltage personnel also trained JWID 04 support personnel on the operation of VIBE products to facilitate the training that would take place the next week. The Voltage personnel would return to Peterson Air Force Base the next week to train the JWID 04 participants on the use of VIBE products while the JWID 04 support personnel would travel to the other sites to train the JWID 04 participants at those sites.

The week of June 7, 2004, Voltage personnel returned to Peterson Air Force Base to train the role player participants in JWID 04 on the operation of the VIBE software. Although the sheer number of concurrent activities that the JWID 04 role players were participating in made the scheduling of the training difficult, the ease of use of the VIBE technology made it extremely easy to fit the required training into the challenging schedule that arose in the training period.

The week of June 7 ended with the JWID 04 role players walking through two days of MSEL events to verify that all of the technologies being tested in JWID 04 were fully operational. In this time period, two of the JWID 04 sites (Dahlgren and DISA Eagle) decided that they needed to bring their own e-mail server on line instead of relying on the capabilities of the server at Peterson Air Force Base. This changed the e-mail addresses of some of the role players in the JWID 04 exercise, and since VIBE cryptographic keys are derived from the user's e-mail address, this caused the need to reissue cryptographic keys to several of the JWID 04 role players. Fortunately, the ease of use of the VIBE technology proved to make this an easy operation.

The remaining two weeks of JWID 04 comprised the actual execution of the MSEL events to exercise the technologies involved in the trials. The MSEL events that used VIBE technology are listed below in Table 1. During the first week of execution, Voltage support engineering received only two support requests, and both of these support requests turned out to be the result of configuration changes by the users (changing settings in Microsoft Outlook). No additional support calls were received in the second week in the execution period of JWID 04.

| UST 01.09 (VIBE) MSEL Events at JWID 04 |     |       |                            |
|-----------------------------------------|-----|-------|----------------------------|
| MSEL #                                  | Day | Time  | Description                |
| 3174                                    | 1   | 14:05 | OSINT Search Request       |
| 3172                                    | 1   | 14:07 | JPEN Report                |
| 3201                                    | 1   | 14:13 | VOI Report                 |
| 3173                                    | 1   | 14:16 | VOI Report                 |
| 3181                                    | 1   | 14:19 | VOI Report                 |
| 3211                                    | 1   | 17:55 | Cross-domain secure e-mail |
|                                         |     |       |                            |
| 3182                                    | 2   | 14:16 | VOI Report                 |
| 3200                                    | 2   | 14:19 | VOI Report                 |
| 3183                                    | 2   | 14:32 | VOI Report                 |
| 3199                                    | 2   | 14:35 | VOI Report                 |
| 3175                                    | 2   | 15:12 | ExPanel Report Available   |
|                                         |     |       |                            |
| 3184                                    | 3   | 14:11 | VOI Report                 |
| 3185                                    | 3   | 15:34 | VOI Report                 |
| 3187                                    | 3   | 15:36 | VOI Report                 |
| 3198                                    | 3   | 16:22 | VOI Report                 |
| 3188                                    | 3   | 16:36 | VOI Report                 |
| 3176                                    | 3   | 17:35 | MI RDD Alert               |
|                                         |     |       |                            |
| 3189                                    | 4   | 14:32 | VOI Report                 |
| 3195                                    | 4   | 14:35 | VOI Report                 |
| 3190                                    | 4   | 15:37 | VOI Report                 |
| 3196                                    | 4   | 15:40 | VOI Report                 |
| 3191                                    | 4   | 16:33 | VOI Report                 |
| 3194                                    | 4   | 16:36 | VOI Report                 |
| 3177                                    | 4   | 17:06 | First Responder SITREP     |
|                                         |     |       |                            |
| 3178                                    | 5   | 15:32 | VOI Report                 |
| 3192                                    | 5   | 15:36 | VOI Report                 |

Table 1: MSEL events exercising VIBE technology in trial UST 01.09.

The execution phase of the UST 01.09 trial consisted of a total of 18 role players, representing the US Navy, US Coast Guard, and various staff elements of USNORTHCOM, who exchanged VIBE encrypted messages, both to and from Microsoft Outlook as well as to and from BlackBerry handheld devices. In each of these cases, all of the clients were required to install VIBE client software.

The execution phase of the UST 02.08 trial consisted of one role player using Microsoft Outlook with the VIBE plug-in installed to communicate securely to other role players who had absolutely no additional client software installed. These additional role players represented the:

- US Army
- Massachusetts National Guard
- Massachusetts State Police



- State of Massachusetts,
- US Department of Justice
- Federal Emergency Management Agency.

This demonstrated the capability of the Zero Download Reader (ZDR), in which an encrypted message is decrypted on a secure server and then presented securely to the client over an encrypted session to a web browser. The presentation of ZDR messages is protected by SSL, the same technology that is used to encrypt credit card numbers sent over the Internet, and is built in to all web browsers.

## *Results and Discussion*

Discussions with the JWID 04 participants before, during, and after the execution phase of the exercise validated that the VIBE technology was extremely easy to use, and provided a way to quickly deploy technology that allowed secure communications, but without the overhead involved with traditional PKI-based solutions. The use of VIBE technology allowed the efficient and rapid deployment of S/MIME security, but without the high costs associated with a full public key infrastructure. The responses to a survey conducted by UST 02.08 are presented in Appendix A.

## *Conclusions*

The JWID 04 exercise provided the opportunity for a number state and federal agencies to test the capabilities of the VIBE technology through a scripted exercise that tested the capabilities of VIBE enabled clients to communicate securely with both VIBE enabled clients as well as clients with no additional software installed. The technology proved simple and easy to use.

## *References*

- [1] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In Proc. Crypto '01, LNCS 2139, pages 213–229, 2001.
- [2] Lt Col Donna L. Warner, USAFR. After Action Report JWID 2004 Regional Threat Analysis Cell (RTAC) US Trial 02.08 “Interagency Information Sharing”

## *Appendix A*

Responses to survey question concerning VIBE technology asked of US Trial 02.08 participants. The following is Page 9 copied from the US Trial 02.08 After Action Report [2]

3. RTAC was partnered with U.S. Trial 01.09 and used the Zero Download email feature of Voltage Identity Based Encryption (VIBE). We have determined all regional participants were able to successfully decrypt data sent from RTAC using VIBE. Does this capability, to send and receive encrypted email without public key infrastructures or the need to download software, have potential utility for your organization’s requirements?

**RESPONSE:**

Very valuable tool and the one that demonstrated the most benefit to the end user. It worked exceptionally well. Little to no train-up was required. No problems were noted with the transmission of data using a multitude of software packages and file extensions. This is a MUST field system.

Daniel McElhinney  
FEMA Region I, Boston, MA

**RESPONSE:**

Definitely. The Coast Guard needs a way to easily distribute security sensitive information with our LE partners at all levels. We also have a requirement to send SSI information to civilian members of our Area Maritime Security Committee.

CDR Dan Ronan  
US Coast Guard, First District (mhs)

**RESPONSE:**

Yes. It was quicker than I expected. I utilize two other systems. This is a good idea if you are going to sign up many agencies vs. just a few. It's a system administrator's nightmare otherwise, e.g. bringing software out to multiple sites for download. Encrypted email is a must in LES circles and many departments would use this as long as 1. Someone else paid for it. 2. It is the one go-to system. Lumping on another system for them to use is not helpful.

Robert Kinney  
MA ATAC

**RESPONSE:**

This has great utility. As mentioned above, the communications were important and, with an issue as sensitive as foreign terrorism situational awareness, security is of utmost importance.

MAJ Eric T. Furey, Commander,  
and CPT Kevin L. Perrin,  
1<sup>st</sup> CST-WMD, Natick, MA

**RESPONSE:**

In short, yes. We would be better able to communicate with partners using something like this.

Detective Lieutenant Michael Cronin  
Massachusetts State Police

**RESPONSE:**

Yes, I found the ease of use, pull not having to download / install software a definite plus.

Barry Wante  
Massachusetts Emergency Management Agency

Appendix B  
Voltage Identity Based Encryption (VIBE)  
For the Creation of Dynamic Coalitions:  
Demonstration of Capabilities at the  
Determined Promise 2004 (DP04) Exercise

## *Abstract*

The initial research that led to the development of a practical Identity Based Encryption (IBE) technology was funded under DARPA's Dynamic Coalitions Program by DARPA contract F30602-99-1-0530. This project led to the invention of Boneh-Franklin IBE [1], the first IBE technology that was found to be both feasible to implement as well as secure. This breakthrough in security technology allows the creation of secure communication channels, but without the burden and overhead associated with traditional public key infrastructure. It accomplishes this by using readily available information, such as a user's e-mail address, as their public key, thus avoiding the traditional problems with public key certification and distribution.

An additional contract, contract FA8750-04-C-0217, was awarded to Voltage Security, Inc., to demonstrate the effectiveness of the technology developed to implement the Boneh-Franklin IBE. This contract provided for the necessary hardware and software needed to demonstrate the Voltage Identity Based Encryption (VIBE) technology, as well as necessary supporting services needed to implement the technology.

The second phase of the demonstration of the Voltage IBE technology took place at the Determined Promise 2004 (DP04) Exercise. At DP04, Voltage Identity Based Encryption technology was installed at USNORTHCOM, at Peterson Air Force Base, and installations at several sites in the States of California and Virginia were also planned in order to facilitate easy and secure communication through e-mail between role players at these sites.

## *Summary*

Determined Promise 2004 (DP04) was a North American Aerospace Defense Command and U.S. Northern Command (USNORTHCOM) homeland defense exercise which ran from August 5-10, 2004. In this exercise, Voltage Identity Based Encryption (VIBE) technology, commercially developed by Voltage Security, Inc., was deployed for operational assessment to both USNORTHCOM, the exercise leader, as well as to exercise participants in the States of California and Virginia. This technology comprised the necessary server software to implement VIBE as well as the client software needed for users to communicate securely.

The server software comprised:

- The Voltage Secure Policy Suite (VSPS), the software product that securely generates and manages the cryptographic keys of the VIBE system.
- The Voltage Enrollment Server, the software product that provides advanced user management functionality for the VSPS product.
- The Zero Download Reader (ZDR) server, the software product that allows users without the Voltage SecureMail plug-in to view and reply to encrypted messages.

The client software comprised the Voltage SecureMail plug-in to Microsoft Outlook that allows a user to both encrypt and decrypt messages using VIBE technology. VIBE protects the email by encrypting it to all authorized recipients. Digital signatures are used to authenticate the origin and content of an email message. Voltage SecureMail leverages S/MIME and VIBE for key exchange, allowing users to encrypt messages without knowing anything beyond the recipient's email address.

The VIBE software was installed and configured to allow the DP04 participants to communicate securely by using e-mail from Microsoft Outlook. Additionally, the Zero Download Reader (ZDR) option was turned on to allow secure communication channels between participants external to USNORTHCOM without the need to install any client software at all.

## *Introduction*

VIBE technology is a breakthrough in encryption technology that allows a user to simply use an identity, such as his e-mail address, as a public key, thus replacing the digital certificates that a traditional X.509 based public key infrastructure (PKI) relies on. Moreover, unlike existing security solutions, secure communication based on VIBE technology can be conducted online as well as offline, from anywhere in the world, without the complexity of certificates, Certificate Revocation Lists (CRLs) and other costly infrastructure.

Traditional X.509 based PKI suffers from several shortcomings, including the difficulty of distributing and using digital certificates, the lack of PKI-enabled applications, and an extremely high total cost of ownership. It is possible to use VIBE technology instead of X.509 based PKI to provide the same benefits to users (confidentiality and integrity of

information, etc.), but at a greatly reduced cost. VIBE technology is easy to implement, scalable and easy to manage, without the overhead and cost inherent in traditional security solutions. By sponsoring the use of VIBE technology in DP04, DARPA hoped to validate the use of VIBE technology to potentially supplement the X.509 based DoD PKI by providing a secure communications mechanism between the DoD and external agencies that are not on DoD PKI.

DP04 tested USNORTHCOM's ability to assist civil and federal authorities in a coordinated response to simulated chemical, radiological, and explosive hazards, and was conducted in the states of California and Virginia. VIBE technology was sponsored by DARPA for participation in DP04 to demonstrate the unique capabilities of the Voltage products to quickly and easily create dynamic coalitions of users, including elements of USNORTHCOM as well as the representatives of the States of California and Virginia, and FEMA Region III and Region IX. The key goal of DP04 was validating the capability of VIBE technology to quickly and easily create a dynamic coalition that could communicate securely, but without the usual overhead and burden associated with using encrypted communications.

Voltage Security, Inc. provided the following technologies for demonstration at DP04:

- Voltage SecurePolicy Suite (VSPS)
- Voltage Enrollment Server
- SecureMail
- SecureFile
- Zero Download Reader (ZDR)

The VIBE Zero Download Reader (ZDR) allows users who receive Voltage SecureMail to view the messages in a web browser, which eliminates the need to install a SecureMail client on the users system. The planned demonstration of the capability of the Zero Download Reader involved the decryption of an encrypted message on a secure server and the presentation of this decrypted message securely to the user over an encrypted session to a web browser. The presentation of Zero Download Reader messages is protected by SSL, the same technology that is used to encrypt credit card numbers sent over the Internet, and is built in to all web browsers.

Functionality that was planned to be exercised at DP04 included:

- Provisioning of private keys to end users after authentication
- End users sending encrypted emails/attachments
- End users receiving encrypted emails/attachments and being able to decrypt them using their private key
- Users who are not authenticated (do not currently have a private key) cannot decrypt emails
- Users read email using the Zero Download Reader (ZDR)
- Instantiation of new users.

## *Methods, Assumptions, and Procedures*

The planning process for the deployment and use of the VIBE software to provide secure communications between the participants in the DP04 exercise began with the First Planning Meeting, held on April 7<sup>th</sup> at the Titan facilities in Colorado Springs, CO. Personnel from Voltage Security participated in the planning meeting with personnel from the USNORTHCOM JCSC Branch (J624), Contingency, Exercise, Training & Planning Branch (J637), and the JWID team within the Information Sharing Branch (J664). This meeting reviewed the requirements and architecture for implementing VIBE for both the JWID04 and DP04 efforts.

A Final Planning Conference (FPC) for DP04 was held in Colorado Springs, CO from 15-17 June, and was attended by personnel from Voltage Security and the USNORTHCOM Contingency, Exercise, Training & Planning Branch (J637). The benefits of VIBE, the experiment architecture, plans and goals were briefed to the Comms Working Group. One-on-one meetings with FEMA, DHS, and DoD personal were held to provide further details on VIBE.

The output of these meetings was an architecture that included two Voltage Secure Policy Suite (VSPS) servers installed at USNORTHCOM.

The architecture that was agreed upon at these meetings is shown below in Figure 6.

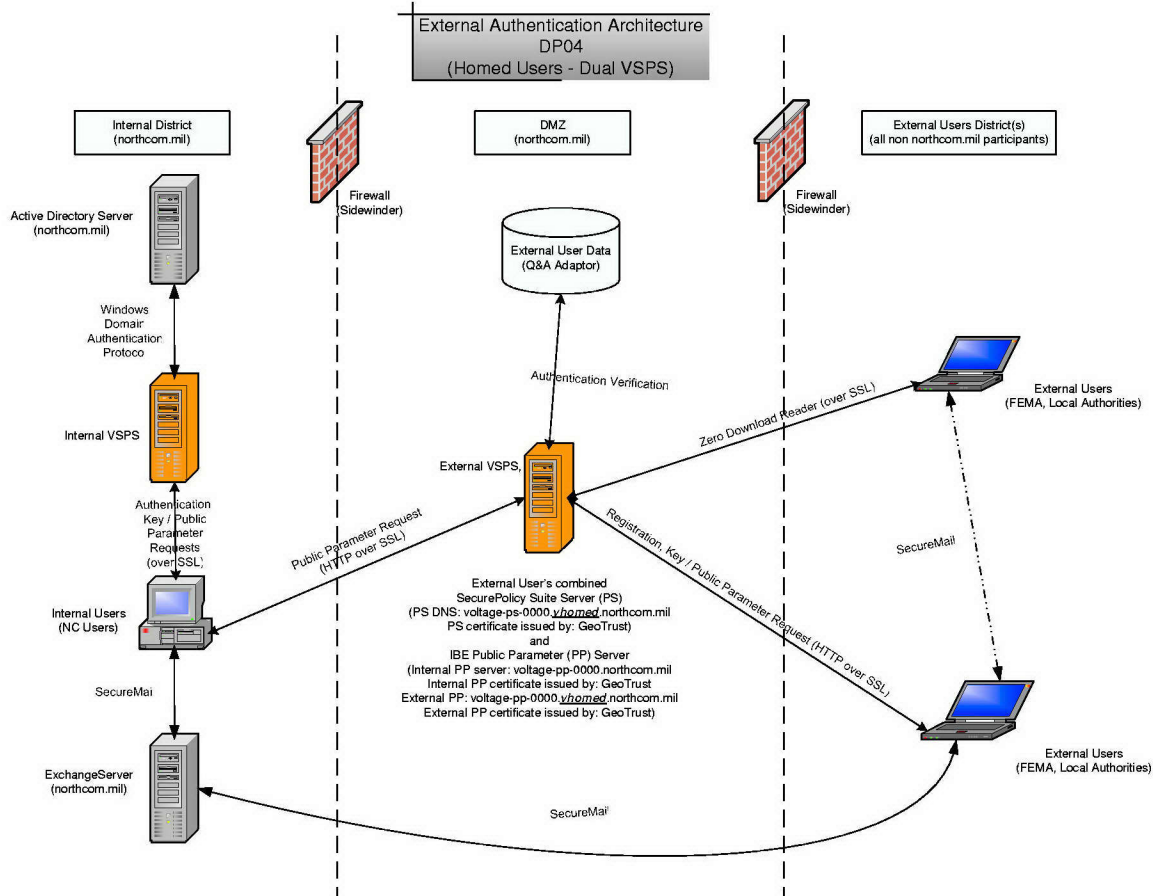


Figure 6: Network architecture for VIBE deployment at DP04.

Figure 6 depicts dual Voltage SecurePolicy Suite (VSPS) servers in the three network zones employed for the VIBE deployment at DP04.

The first zone, Internal District (northcom.mil), contained the Active Directory server, internal users' Voltage SecurePolicy Suite Server, Voltage Public Parameters Server, and internal users. The second zone, DMZ, contained the Q&A adaptor (used to authenticate external users), external users' Voltage SecurePolicy Suite Server, Voltage Public Parameters Server. The third zone, External Users' District (external.northcom.mil), represented all non-USNORTHCOM participants, such as FEMA.

The location of Voltage SecureMail users has an impact on the number and the location of the VSPS server. The DP04 participants using SecureMail are on different LANs and the environment is set up to accommodate external users. As a result, a single VSPS on the internal network is not sufficient to accommodate all users. The dual VSPS configuration as shown in Figure 6 is the best approach for this deployment scenario and has a number of advantages.



In order for external users to send secure e-mail to people inside an organization, the enterprise's public parameters must be made available on a publicly accessible server, such as in the DMZ. The internal VSPS server is used for DP04 internal users on USNORTHCOM internal LAN while the VSPS server in the DMZ is used to support DP04 external users such as those from FEMA. In this configuration, all internal communications will use the internal VSPS server, while communications with external users will utilize the VSPS server in the DMZ.

The DP04 deployment configuration enables two separate districts – one on each VSPS server, each with its own Master Secret. This provides better performance and availability, and offers the additional benefit of setting up separate security domains for internal classified communications and external sensitive communications. If the Master Secret on the external VSPS server is ever compromised, internal communication using the internal VSPS is still secure.

The full network connectivity for the VIBE deployment at DP04 is shown below in Figure 7.

## Internet Connectivity for DP04

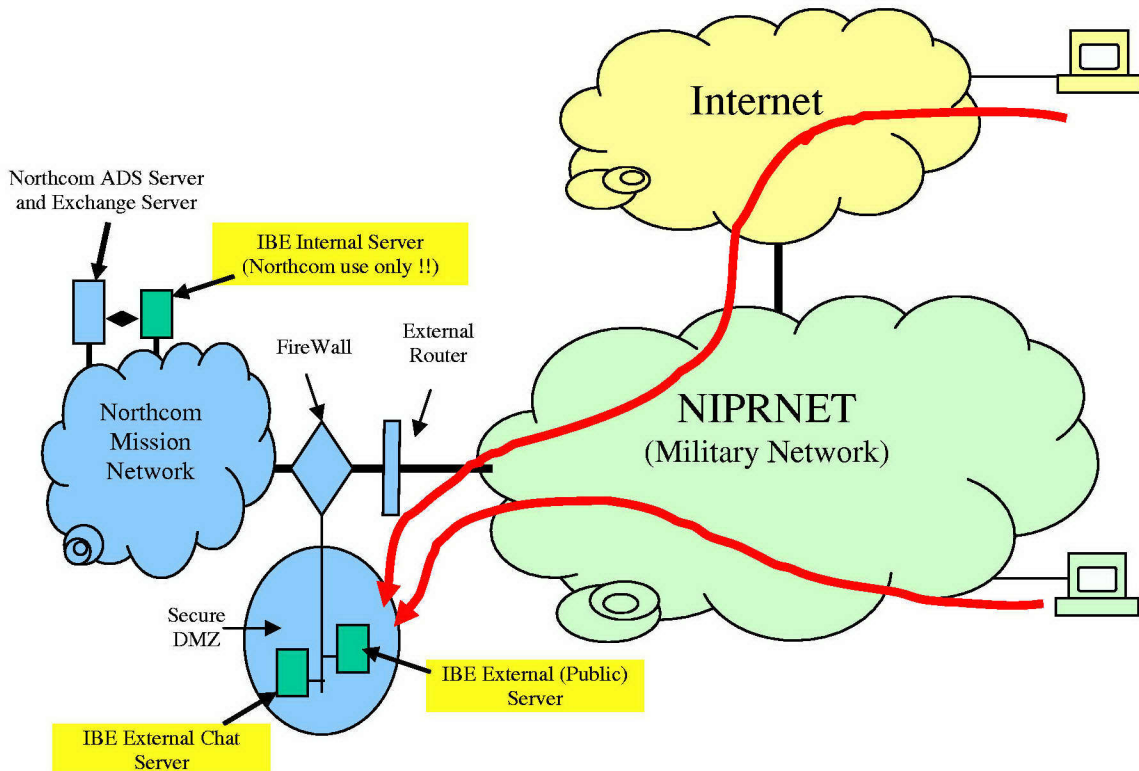


Figure 7: Network connectivity for the VIBE deployment at DP04.

Based on the planning meetings, the following were provided to the DP04 personnel:

- Hardware requirements list
- VIBE software required for the VIBE deployment
- Planning, Installation and Administration guides for the VIBE deployment
- Configuration worksheets detailing the configuration required for the approved operation of the VIBE software for DP04. This includes the IP address and SSL certificates configuration, district configuration, ID management for authenticating both internal and homed users, and client policy settings for the local users.
- Printed documentation of the VIBE technology to be made available to the DP04 participants and role players.

After the completion of the DP04 planning meetings, continuous coordination between Voltage personnel and DP04 personnel ensured that the necessary hardware and software required for the implementation at DP04 was delivered as required, and that printed documentation on Voltage VIBE technology was available to DP04 participants during the exercise execution.

Also following the DP04 planning meetings, extensive testing was performed by Voltage Security, Inc. engineers to ensure that the capabilities to be tested in DP04 would meet the usability needs of the DP04 role players. Product configuration refinements were completed during this period, and extensive work to make the user interface as easy to use as possible without compromising security was performed.

Voltage personnel visited Peterson Air Force Base on July 20-21 to participate in the DP04 set-up activities. The VIBE servers were installed during this visit. The configuration of these servers was also started but could not be completed due to unavailability of the backup of the VIBE pilot server from UD04. This backup was required to recover the key store to set up the web server, hosting the public parameters for the internal server, in the DMZ. Also during this visit, Voltage personnel provided the USNORTHCOM JCSC personnel with the Voltage SecureMail client on a CD and also instructions and training on how to install and use client software.

Voltage personnel revisited Peterson Air Force Base on July 29-30 to complete the configuration of the VIBE software. During this visit, a meeting was convened on July 30<sup>th</sup> to obtain CCB approval and revalidate the IATO for the VIBE deployment. The VIBE server software configuration could not be started until this approval was received. Voltage personnel were allowed to continue the configuration of the VIBE servers on July 30<sup>th</sup>.

The VIBE deployment was complete as of August 4<sup>th</sup>. Information about the Voltage Technical support was provided. This included a 24x7 support number that is always manned by a human being. This person can triage problems and contact the appropriate Voltage engineer to expedite the resolution of the issue. This support capability is especially useful during non-business hours. Information was also provided to setup

access to the Voltage Solutions Portal which allows the user to search the Voltage knowledgebase, submit help requests, and check on the status of existing support issues.

The training of the participants in DP04 on the operation of the VIBE software was planned to be handled by USNORTHCOM J6 personnel.

## *Results and Discussion*

DP04 started on August 5<sup>th</sup> and ran through the 10<sup>th</sup>. The VIBE server software was fully deployed and functional as of August 4<sup>th</sup>. The VIBE technology was tested for readiness the day before the start of the DP04 exercises. The client was downloaded by both an internal user and a user from Voltage acting as an external participant to verify that the software was correctly set up and that the test participants could communicate securely using VIBE technology.

The Voltage personnel provided the USNORTHCOM JCSC personnel with client CDs and instructions on how to install the SecureMail client on the workstations of internal participants. Additionally, the USNORTHCOM JCSC personnel were also given instructions for the external participants to download the SecureMail client from the client download page hosted on the VIBE server in the DMZ.

Communication with the USNORTHCOM personnel during the DP04 exercises was severely limited. As of the end of the exercises on the 10<sup>th</sup>, no confirmation could be obtained from the USNORTHCOM J6 as to how many SecureMail clients were installed and how much usage the VIBE technology received.

The assessment fell short of what was originally intended. There were some unforeseeable issues that came up that were beyond everyone's control. The USNORTHCOM Server Room experienced flooding during the DP04 exercises as a result of flash flooding in Colorado Springs. This did delay the roll out of the SecureMail clients and perhaps the usage of VIBE at DP04.

## *Conclusions*

The VIBE servers were successfully configured and deployed at USNORTHCOM to support DP04 usage. The deployment was tested by personnel from both USNORTHCOM JCSC and Voltage Security to ensure that DP04 participants would be able to communicate securely with each other. USNORTHCOM maintains strict configuration control over user workstations and exercise participants did not have necessary permissions to download and install software. As a result, members of USNORTHCOM's Joint Communications Support Center (JCSC) were tasked with installing the VIBE SecureMail client software on each participating exercise workstation. Due to circumstances that were beyond everyone's control this client software installation never took place, preventing exercise participants from using VIBE to encrypt and decrypt messages during the execution of the exercise scenario.

Even though the assessment of the VIBE software fell short of what was originally intended, the positive feedback from the UD04 and the JWID04 exercises has shown that the VIBE technology is a viable solution for supporting secure communications between diverse communities of interest where common authentication methods, such as PKI, are not shared.

## *References*

- [1] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In Proc. Crypto '01, LNCS 2139, pages 213–229, 2001.