



# Method for establishing secure real-time Virtual Peer-to-Peer communications

VERSION 1.4

October 2, 2003

# Table of Contents

**TABLE OF CONTENTS..... 2**

    TABLE OF FIGURES..... 3

    LIST OF TABLES..... 3

    TECHNICAL FIELD..... 3

    KEY WORDS..... 3

**TERMINOLOGY..... 4**

**ABSTRACT..... 5**

**INTRODUCTION..... 6**

**VIRTUAL PEER-TO-PEER MODEL..... 7**

    TRADITIONAL MODES OF COMMUNICATION..... 7

    SUMMARY OF IX COMMUNICATION MODES ..... 10

    DIFFICULTIES WITH INTERNET B2B INFORMATION EXCHANGES ..... 10

    THE CHALLENGE..... 11

    ENTER THE SECURE VIRTUAL TUNNEL (SVT) ..... 11

    PEER-TO-PEER WITHOUT SVT..... 12

    HUB NETWORK UTILIZING THE SVTs..... 14

    SVTs ARE ADDITIVE..... 15

**PUTTING IT ALL TOGETHER..... 16**

    PROCESS FLOW..... 18

**IMPLEMENTATION..... 19**

    ESTABLISHING TRUST..... 19

    SECURE VIRTUAL TUNNEL IMPLEMENTATION..... 23

    VP2P IMPLEMENTATION..... 25

**CONCLUSION..... 27**

**APPENDIX A: RELEVANT PATENTS AND PATENT APPLICATIONS..... 28**

**APPENDIX B: REFERENCES..... 29**

***Table of Figures***

**FIGURE 1 - CENTRAL 'HUB' OR VALUE ADDED NETWORK.....7**

**FIGURE 2 - NETWORK INTERCONNECTS..... 8**

**FIGURE 3 - FULLY CONNECTED POINT-TO-POINT NETWORK CONFIGURATION.....9**

**FIGURE 4 - INTERNET-BASED FULLY CONNECTED NETWORK CONFIGURATION..... 9**

**FIGURE 5 – DIRECT PEER-TO-PEER COMMUNICATION.....13**

**FIGURE 6 – SVT SUPPORTED CENTRAL NETWORK COMMUNICATIONS..... 14**

**FIGURE 7 - STEPS TO ESTABLISH VIRTUAL PEER-TO-PEER COMMUNICATIONS.....17**

**FIGURE 8 - SIMPLIFIED VIEW OF VIRTUAL PEER-TO-PEER COMMUNICATION..... 18**

**FIGURE 9 - ESTABLISHMENT OF A SECURE VIRTUAL TUNNEL..... 23**

**FIGURE 10 - DIFFERENT PROTOCOL SUPPORT OVER MULTIPLE SECURE VIRTUAL TUNNELS.....24**

***List of Tables***

**TABLE 1 - TERMINOLOGY..... 4**

**TABLE 2 – COMMUNICATION MODE ATTRIBUTES.....10**

**TABLE 3 – PORT INFORMATION TO SUPPORT VIRTUAL PEER-TO-PEER COMMUNICATION..... 26**

***Technical Field***

Secure communications over an insecure network.

***Key Words***

Information exchange, business-to-business, security, communication protocols, real-time communications, routing

## Terminology

The table below defines some of the terms discussed in more detail in this document.

Authentication	The process of identifying an individual or system. For users, it is usually based on a username and password. For systems, certificate based authentication is often used.
Authorization	The process of granting or denying access to a network or system resource.
Central Node	A system involved in an information exchange that is neither the originator nor the final destination of the communication.
Firewall	A system designed to prevent unauthorized access to or from a private network.
HyperText Transfer Protocol (HTTP/HTTPS)	The underlying protocol used by the World Wide Web. HTTPS is a secure version of the protocol.
Information Exchange (iX)	Movement of data between 2 or more business partners. Business-to-business information exchange is often abbreviated as B2BiX.
Interconnect	The capability that allows one third party network to communicate with another. Most EDI third party service providers offer network interconnect capabilities.
Peer-to-peer (p2p)	Communication between two end points without routing/processing by a third party or central node.
Remote Node	An endpoint in an information exchange. A Remote Node is either the originator or the final destination for the information exchange.
Secure Shell (SSH)	A program and protocol used to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels.
Secure Virtual Tunnel (SVT)	Communications mechanism that provides the ability to 'tunnel' or 'encapsulate' another protocol within an established secure session.
Value Added Network (VAN)	An EDI third party service provider.
Virtual Peer-to-Peer (Vp2p)	A communications mechanism having the ability to provide real-time secure communications via a central proxy server.

**Table 1 - Terminology**

## Abstract

This document describes a number of innovations that accomplish the declared purpose better than existing methodologies. That purpose being the establishment, management and use of secure real-time communication provisioning for the express purpose of exchanging information between two parties over an insecure network. In particular, this paper will focus on the use of these mechanisms to exchange information between two business partners.

The paper establishes a brief history of the mechanisms that have been used to exchange information between two parties. This provides a summary of some of the key technologies that have been employed as well as recognizing some of their strengths and weaknesses.

This is followed by a section that details the innovations that provide a the building blocks for achieving the information exchange and details the benefits of each of the new mechanisms.

The next section demonstrates how these new mechanisms are used in combination to achieve the overall goal of secure real-time information exchange over an insecure network.

Following this is a section that details one implementation of the described innovations. Lastly is a conclusion section that summarizes and emphasizes the salient points of this paper.

## Introduction

There have always been mechanisms to transfer information from one business to another. Over time, these have ranged from grunts, speech, smoke signals, telegraph, telephone, EDI [1], fax, email and now electronic information exchange via the Internet. Each new type of communication method and protocol has had its own set of challenges, and Internet-based information exchange certainly comes with its own set of issues. Among these are:

- the ability to distinguish and allow communication only with trusted businesses and/or individuals within the businesses
- securing the information such that only appropriate businesses and/or individuals within the businesses receive and/or have access to the information, and
- the ability to manage these communications while both the business and technical environments continue to change such as adding new business partners and the adoption of new protocols on the Internet itself.

Prior to the Internet, many electronic communications were either handled using direct (peer-to-peer) or trusted third party (hub) models. These models avoid the problems noted above quite well. However, ultimately, the ubiquity of the Internet is winning more and more converts in the communication arena due to many factors including price, standardization, universality, and functional capabilities. This move towards Internet-based information exchange requires new mechanisms to solve business-to-business information exchange (B2BiX).

One possible solution to this quandary is to use a hub model on the Internet where a single company is the central connection point for all information exchanges between business partners. This provides a good compromise by using the ubiquity of the Internet and the well-accepted communication protocols, but maintains a certain level of security and manageability by centralizing these functions. However, there are additional costs involved with the hub model. Now, rather than using the distributed nature of the Internet to share expenses, a single entity takes on a hefty portion of the expenses by routing all traffic through their own infrastructure. The added expense makes the hub solution less than ideal.

Internet-based peer-to-peer communication provides a robust mechanism for handling B2BiX. Under this model, all communication is direct between the two Remote Nodes, without a Central Node to direct and route traffic. However, peer-to-peer communication also has limitations, such as the need to configure communication between each node, security vulnerabilities, and management overhead such as the maintenance of configuration settings when IP addresses change at any node.

These facts created the impetus for the creation of the Virtual Peer-to-Peer model (Vp2p). Vp2p was created to address the following challenge:

**Make peer-to-peer communications at least as secure as centralized, hub-based network communications while minimizing the cost associated with configuring and maintaining these communications.**