Skype

Guide for Network Administrators

Skype 3.0 Beta

The whole world can talk for free. Skype.com

© Skype Limited 2006

What is this Guide?

This guide provides information to help you understand how Skype works, how secure Skype is, and how to manage Skype in the context of an enterprise environment.

Who should read this guide?

This beta draft of the new and improved *Network Administrator's Guide* is for IT personnel like yourself (system and network administrators) who are responsible for managing the deployment of software applications, specifically on the Microsoft Windows Platform.

The guide is intended to help you understand the Skype architecture and security model, and to provide newly released information on how to install and configure Skype in enterprise settings.

This *Network Administrator's Guide* assumes you are familiar with enterprise deployment issues, editing the Windows registry, Windows Group Policy Administration, basic XML syntax, as well as other things related to networking and operating system environments.

How to read this guide

This document uses the following text conventions:

Format	Indicates
UPPERCASE	keyword such as an object, a command, or a notification
`lowercase`	category of a keyword, such as CALL duration
`<angular_brackets>`	identifier, such as a username or a call ID
`[<square_brackets>]`	optional items
`* (asterisk)`	repetitive items
`|(vertical bar)`	or
`->`	command issued by client
`<-`	response or notification from Skype
`//`	comment in code example
`>`	select next menu item

Important legal information

Before distributing Skype, or using the Skype API, please ensure you clearly understand the legal terms and agree with them. You will find these documents on the Skype website and/or accessible from the Skype client.

- Like all Skype users, you must sign the **End User License Agreement**. `http://www.skype.com/company/legal/eula/`
- To redistribute Skype you must agree to the **API redistribution terms.** `http://www.skype.com/company/legal/terms/api_redist.html`

Copyright

This document is the property of Skype Technologies S.A., and its affiliated companies (Skype), and is protected by copyright and other intellectual property rights laws in Luxembourg and abroad.

Skype makes no representation or warranty as to the accuracy, completeness, condition, suitability, or performance of the document or related documents or their content, and shall have no liability whatsoever to any party resulting from the use of any of such documents.

By using this document and any related documents, the recipient acknowledges Skype's intellectual property rights thereto and agrees to the terms above, and shall be liable to Skype for any breach thereof.

Trademarks

Skype is a trademark of Skype Technologies S.A., in Luxembourg and other countries. Windows is a registered trademark of Microsoft Corporation in the United States and other countries. Linux is a registered trademark of Linus Torvalds. Apple and Macintosh are registered trademarks of Apple Computer, Inc., in the United States and other countries.

All other names or brands may be trademarks or registered trademarks belonging to their respective owners.

Disclaimer

This document describes services offered by Skype Technologies S.A., its subsidiaries or affiliates as of the time of this writing. Skype services may be modified or terminated at any time according to the current Skype Terms of Service available at the official Skype website. The internal design of Skype software and networking techniques are subject to change without prior notice.

Skype is not responsible for the content of any third-party websites or documents that may be referenced in this document. Any such references are provided purely for the convenience of Skype's customers, who are advised that Skype has not verified that such references are accurate or fit for any particular purpose.

What is in this Guide?

What is this Guide? 2
Who should reads this guide? 2
How to read this guide 2
Important legal information 3
Copyright 3
Trademarks 3
Disclaimer 3
What is in this Guide? 4
Overview 5
Description of Skype Services 5
Other information 6

INTRODUCTION
What Every IT Manager Should Know 7

HOW SKYPE WORKS
Skype P2P Architecture 8
Intelligent Routing with Supernodes 8
Skype Supernodes and Relay Hosts 9
Skype Client / Supernode Relationship 10
Skype Global Index 10
Firewall and NAT-Device Traversal 11
Skype Network Resource Consumption 11
Bandwidth Indicator 11

SKYPE SECURITY MODEL
Skype User Authentication 13
How are Skype Sessions Established? 14
How Is Encryption Handled? 15
Security & File Transfers (Viruses, Trojan Horses, etc.) 16
Anti-Virus Shields and Real-time Scanning 17
Privacy and Sharing Contact Details 19
An Example - Sharing Contact Details 19
Blocking Other Skype Users 20
Preventing "spam" and "spit" 21
How to Prevent Phishing 21
Where Does Skype Store Data? 22
Files, Folders, & Application Data Locations 23
Passwords 24
Adware and Spyware 24
Skype Security Evaluation 25
Skype Security FAQ 25
Is "Hole Punching" a Security Issue? 25
How Secure is the Skype telephony connection? 26
Are Skype Users at Risk of Trojan Viruses and Other Threats? 27

DEPLOYING SKYPE IN THE ENTERPRISE
First things first 29
General Guidelines 29
How to Determine if your Network is Skype-Friendly? 30
Verifying the Authenticity of the Skype Installer for Windows 30
Problems with a Digital Signature 31
Skype Client Notifications for New Versions and Updates 32
Enterprise-wide Installation and Setting Policies 33
Policies 33
Setting Up Group Policies 34
Configurable Policies 34
Registry Keys 36

Overview

The Skype software and services provide people with a new, secure and innovative way to communicate with other people using the Internet as the medium of transport for messages, whether through voice calls, text messages or other forms of communication.

Skype is the world's first decentralized telephony network, but it provides far more services than just voice calling carried over the public Internet.

By using a compact client program (which is available in versions for several popular computer platforms) a Skype user is able to send or receive text messages, hold voice calls and exchange data files with other persons using Skype.

Communications with other on-line Skype users are provided free of charge, while certain premium services, such as the placing of voice calls to standard telephone numbers, are available for a modest fee.

Skype communications rely largely on peer-to-peer communications techniques in order to improve the quality of voice calls and to reduce the latency of data transfers between users.

The term "peer-to-peer," frequently written as "P2P," is a class of software applications that rely on resources located at the network edge, such as the large number of individual personal computers that are always connected to the Internet, rather than relying on large and costly centralized computer servers. It's this aspect of Skype networking that makes it robust and tolerant of network failures. Skype has no single "critical node" upon which the service relies for its operation.

Description of Skype Services

The utility of Skype services are found in the voice and video calling, file transfer and instant messaging facilities that are built into every user Skype software client. Underlying these services are Skype's directory, presence management and network traversal technologies.

Skype provides its users with a variety of communications and related services, including the following:

- Voice calling other Skype user(s)
- Voice conference calling
- Voice calling to traditional telephone lines (SkypeOut)
- Voice calling from traditional telephone lines (SkypeIn)
- Making video calls
- Chat, providing instant messaging for groups of up to 48 participants
- Cross-platform file transfers
- Directory and presence management

Skype user programs have been built for use on several popular computing platforms, including, but not limited to, personal computers running Windows XP, Windows 2000 or Linux, Apple Macintosh computers running Mac OS X and Pocket PCs running Windows Mobile.

Other information

Here is a list of external resources referenced in this guide:

- **Using Administrative Template Files with Registry-Based Group Policy**
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/gp/admtgp.mspx

- **Open Group Policy as an MMC Snap-in**
  http://technet2.microsoft.com/WindowsServer/en/library/ae13960b-3a27-4b19-a866-ed6e6e7a312d1033.mspx?mfr=true

Introduction

Increasingly, large organizations and enterprises are choosing to allow Skype to run on their networks to benefit from the dramatic cost savings, secure file transfer capability, multi-chat communications ability, and other productive features.

What Every IT Manager Should Know

Skype Technologies S.A., wants people to enjoy using Skype in the enterprise as much as they do at home.

The Skype development staff is constantly focusing on improving ease of use, and with each subsequent release, the Skype client is becoming more full featured; both for use at home and now for deployment across the enterprise.

Following are some key points to share with IT management so they know that Skype is becoming increasingly IT friendly:

- **Skype saves money** – With zero per-client costs and favorable outbound calling prices, Skype can slash your enterprise communication costs.
- **Skype is secure –** Information traveling over the Skype P2P network is completely secure.
- **Works with antivirus tools -** Inbound and outbound Skype file transfers are scanned by the major antivirus products.
- **Protects privacy –** Skype's encryption and authentication may help you meet enterprise and national privacy mandates.
- **Firewalls stay secure** Skype doesn't require any inbound openings in your firewalls – often no change is needed at all.
- **Skype gives you control –** You can turn off or configure a variety of Skype's functionality or settings, including file transfer and the API.
- **Users are protected from SPAM** – Permission-based communication disallows most unwanted communication.
- **No adware or spyware** – Neither the Skype client nor the Skype installer installs any software without the user's consent.

How Skype Works

Instead of relying on centralized infrastructure and equipment, Skype relies on state-of-the-art P2P networking technology to establish connections among Skype clients, as well as to route calls, IMs, file transfers, and video between one Skype client and another.

Once installed, Skype is similar to any piece of end-user software. The Skype client runs in the foreground while the user is making voice and/or video calls, sending/receiving IMs, transferring files, etc. it. Otherwise, the Skype client runs in background, consuming minimal computer and networking resources.

Skype P2P Architecture

Interaction between any pair of Skype users – any combination of voice, video, text chat, or file transfer – are carried over an encrypted "session layer" that is established among the communicating Skype users before messaging begins.

The Skype solution is composed of the Skype client and the underlying P2P network. The Skype client is primarily a communications platform, and it also offers other essential capabilities that integrate voice calling, instant messaging, person-to-person videoconferencing, and file transfers into one seamless program.

The Skype client is tightly coupled to the underlying network and relies on an authentication server, which is discussed in more detail later. And, unlike many P2P applications, the Skype client (when downloaded from the Skype website) does *not* contain any adware, malware, or spyware.

Intelligent Routing with Supernodes

When a Skype client is downloaded and installed, a user's computer becomes part of the Skype P2P network, which is composed of Skype network peer nodes, supernodes, and relay hosts. Skype's ability to act as a self-forming distributed network is the result of the interaction among ordinary nodes, supernodes, and relay hosts throughout the network.

A *supernode* is a regular Skype peer node that, under a particular set of circumstances, takes on additional responsibilities. Supernodes are responsible for detecting Skype clients that are online, establishing connections among them, and transmitting signaling messages to ensure encrypted traffic is routed efficiently.

Supernodes work in concert with one another to support the Skype directory service or *global index*—a distributed database of Skype users. The Skype global index is, in part, composed of a hierarchical system of available supernodes. See, "Skype Global Index" later in this document for more information on supernodes.

The global index is not hosted on central servers. When a capable computer with a high-speed connection to the Internet runs the Skype software, under certain circumstances, it may automatically "come alive" as a supernode, and function as a temporary directory index server for nearby Skype clients. Each supernode's capabilities are based on the computer's available memory, bandwidth, and uptime characteristics.

Only a relatively small percentage of Skype nodes ever transform into supernodes, even though supernode capabilities are built into every Skype client.

Where do the supernode's additional capabilities come from? When the Skype client is installed, only part of the application is visible to the end user. In addition to the portion of the Skype client which the end user can see, the Skype software installation includes functionality that evaluates the capabilities of the computer on which Skype is installed, as well as its network connection to identify how capable the new resource might be to the Skype network.

Under normal circumstances, a Skype client functions as an ordinary node in the Skype network. However, a Skype client that is running on a high-performance computer with a healthy connection directly to the Internet may, under certain conditions, "wake up" to support the global index by acting as a supernode or relay host thus giving the Skype network minor but essential additional capabilities above and beyond the simple capabilities that end users are aware they actually need.

Skype Supernodes and Relay Hosts

When a Skype peer node comes alive as a supernode, it dynamically creates a local cluster in a star-like pattern of up to several hundred peer nodes to leverage all the available resources on the Skype P2P network.

Each supernodes holds the directory entries of up to several hundred Skype users. And although supernodes need to accept a relatively small number of directory queries, they do not actually carry content: voice, text, video, or file-transfer data. Supernodes are restricted from using more than 5 kilobits per second of bandwidth.

Type of Traffic	Bandwidth Limit Per Session
Signaling Info	5 Kbyte per second (strict)

Table 1. Supernode Bandwidth Limits Per Session

A relay host is similar to a supernode but is has a different role and purpose in the Skype network. While each supernode functions as temporary directory index server for nearby peer nodes in the cluster, a relay hosts acts as data-transfer *relay* station by connecting Skype clients that are unable to connect directly with one another.

Relay hosts *do* carry Skype network traffic but they have strict limits in terms of how much bandwidth they can consume on a per-session basis. Note also, that while in theory a relay host can carry more than one relayed session, in practice this is uncommon and shouldn't have an impact on capacity planning.

Type of Traffic	Bandwidth Limits Per Session
File Transfer	3 Kbyte per second (strict)
Voice call	4 kByte per second
Video call	10 kByte per second (strict)

Table 2. Relay Host Per-Session Bandwidth Limits

The computing resources required to support the activities of a supernode or relay host are small compared with relative processing power, memory, storage space, and available bandwidth on a given computer.

In addition, given the strict bandwidth limits placed on supernodes and relay hosts, Skype end users cannot tell the difference between a given computer being used as a regular Skype node, supernode, or relay host because the capabilities required to support the additional functionality are transparent and have no noticeable impact on a given computer's performance.

Skype Client / Supernode Relationship

Every Skype client stores a list of supernode network addresses that allow a peer node to connect with the network. When a Skype client successfully contacts a working supernode, the Skype client gets an updated list of network addresses of currently active supernodes for future use.

The Skype client selects an active supernode as its "upstream" link and then uploads search requests and other relevant data to this supernode. This supernode, in turn communicates with other supernodes to satisfy any search request. Search requests might be an authorization, a voice or video call, IM, or a file-transfer request. Skype clients always first attempt to communicate with other Skype clients directly.

When it is impossible for a given Skype client to communicate with another Skype client directly, the active supernode routes the connection and call traffic through a relay host.

Each Skype client opens multiple standby connection paths and then dynamically chooses the path with the lowest latency and optimal bandwidth to increase call-completion rates and improve overall service quality. The Skype client then connects to a peer node and transfers text, voice, file transfer data, and video using Hypertext Transfer Protocol (HTTP).

The Skype client maintains multiple connections even if it's not a supernode. As a result, you may see a large number of TPC/UDP connections, even when a Skype client is not a supernode or relay host.

Important Note: Certain inexpensive routers, firewalls, or gateways (generally designed for home use and not certified by Skype) may fail to support the number of concurrent TCP/UDP connections required to ensure high call completion rates and call quality.

Skype Global Index

Prior to Skype version 1.2, user Contact Lists were maintained in each individual's Skype client (on a given computer). A centralized directory for managing Contact Lists was added at version 1.2 of the Skype client to ensure that users' Contact Lists are available on any computer when they log in to Skype.

This means that you can deploy new computers (or let users work from multiple computers) while retaining access to Contacts Lists when the users are logged in.

More recently, the now *de*centralized directory service or *global index* was deployed to enhance the overall quality of the end user experience. As mentioned previously, the global index is not hosted on central servers and is, instead, maintained as a hierarchical arrangement of all available supernodes.

Firewall and NAT-Device Traversal

In most situations, Skype automatically traverses the vast majority of firewall and NAT boundaries. Therefore, many of the problems that network administrators encounter when they attempt to deploy SIP (Session Initiation Protocol)-based Internet voice solutions are often avoided by Skype's innovative P2P network architecture.

Skype clients on publicly routable Internet addresses (and those that are not behind restrictive firewalls) can provide assistance to peer nodes that are hindered by network address translation.

The ability of peer nodes outside a firewall to assist peer nodes behind a firewall or NAT allows Skype clients to connect, as long as they both can make an outgoing connection to the Internet.

As a result, when a user initiates a Skype call, the connection can be made, regardless of whether the caller or the recipient is behind a firewall or a NAT boundary.

It is true that some software firewalls interfere with Skype, however. In such cases, you can simply reconfigure the software firewall to allow the Skype client to work.

Skype supports regular HTTP or HTTPS proxies, and authenticating HTTPS/SSL and SOCKS5 proxies. In the Skype client, these preferences can be set through the Tools -> Options - > Connection.

Skype Network Resource Consumption

Generally, Skype peer nodes, supernodes, and relay nodes require minimal CPU cycles. And, with the exception of additional processing power needed for conference calls, and bandwidth required for large file transfers, resource requirements are minimal, even for video calls.

Bandwidth Indicator

The Skype Windows client now supports a visual bandwidth indicator, which is turned off by default. When the bandwidth indicator is turned on, a visual display replaces the on-line status text in the lower left-hand area of the Skype main window to provide a window into how much bandwidth Skype is using, both for upload and for download.

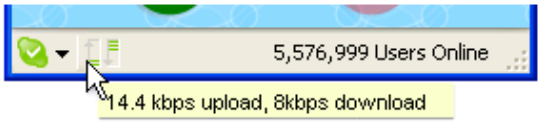

Figure 1. Skype Client Bandwidth Meter

The bandwidth indicator is composed of seven colored bars, which move up and down according to the amount of bandwidth being used.

Each bar in the bandwidth indicator represents a bandwidth threshold. The bars are colored green, yellow, or red depending on the amount of bandwidth being consumed.

Bar 7	150kbs
Bar 6	125kbs
Bar 5	100kbs
Bar 4	75kbs
Bar 3	50kbs
Bar 2	25kbs
Bar 1	0kbs

Table 3. Skype Client Bandwidth Meter Thresholds

The visual bandwidth indicator is "off" by default. However, you can turn it on as a preference settings. Go to Tools -> Options -> Advanced and put a checkmark in the box to "Display Skype bandwidth usage.

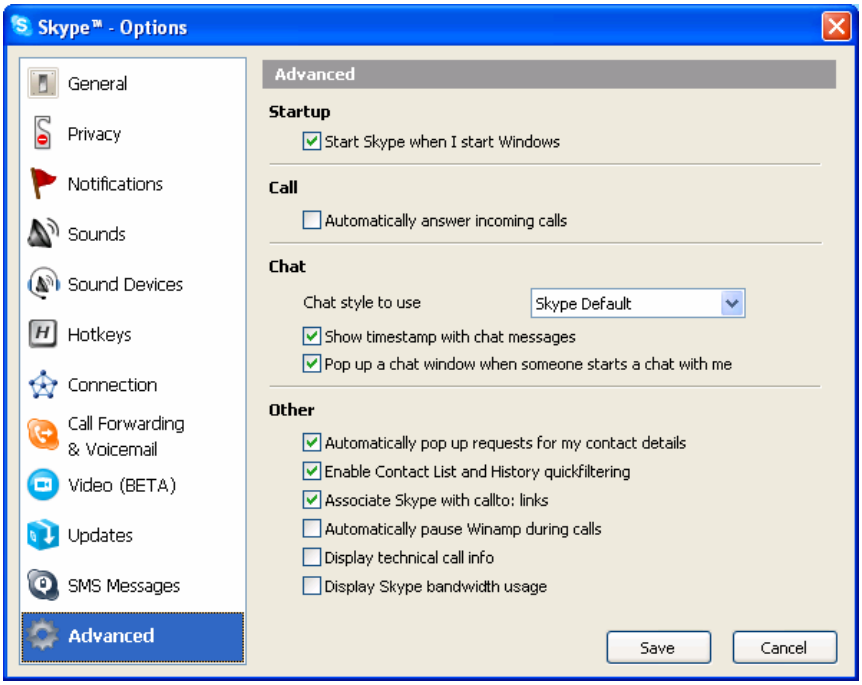

Figure 2. Skype Client Bandwidth Meter Preference

Skype Security Model

Skype is the only Internet voice application provider that currently employs strong encryption to protect network traffic. This is because Skype's tight security model is integrally linked to its underlying P2P network architecture.

The fact that Skype network traffic is routed through supernodes and may be routed through relay hosts (computers and devices that are not party to a call, IM, or file transfer) means that all Skype network traffic must be automatically encrypted end-to-end to ensure privacy.

As a result, Skype's network traffic cannot be intercepted and decoded while in transit. That being said, even though Skype offers a private communication channel, it still runs on mass-market operating systems.

This means that even though Skype network traffic cannot be intercepted and decoded while *in transit*, when Skype traffic is decrypted on computers that are party to a call, IM, or file transfer, data such as chat logs, and voicemail messages may be vulnerable.

In the context of the security provided by operating system(s) on which the Skype client is installed and running, Skype provides operational level of security or privacy. Therefore, Skype neither provides a secure computing platform in the strictest definition, nor does it offer a secure file storage solution.

By *secure computing platform*, we mean a computing platform that meets technical criteria about how information is transmitted, received, handled, and stored such that high-value or high-risk transactions can be handled securely.

Skype utilizes a security model that effectively prevents anyone who may have access to a supernode or relay host from interfering with or capturing any part of a Skype communication, even if they are able to collect or sniff network data packets. It also prevents anybody (especially those you consider to be a competitive threat) from installing a computer on the Internet in the theoretical path of incoming and outgoing Skype traffic for the purpose of eavesdropping.

The bottom line is this; although Skype cannot guarantee complete anonymity or secrecy, it does provide transport-layer security to ensure that message content traveling over the Skype network cannot be tapped or intercepted. Skype network traffic and message content will not end up at unauthorized destinations.

Skype User Authentication

Skype's security model utilizes a public-key cryptography with signed digital credentials. This enables Skype to validate each user's authenticity. It also reduces the demand for centralized infrastructure.

With public-key/private-key cryptography, one of the keys is made "public" enabling unrestricted distribution. However, the other key remains secret. The two keys are independent but related. Neither of the keys can be used to predict what the other key is. Both keys are needed to complete the handshake that allows a given communication session to complete.

When a Skype user logs in using a Skype name and password, the user's Skype client attempts to connect to a centralized resource; that is, the Skype authentication server. If and when the authentication server validates the connection, it gives the user's Skype client a signed digital credential—signed using a private key which is maintained by Skype Technologies S.A.

The public key required to verify another Skype user's digital credential is maintained in each Skype client. Signed digital credentials are valid for only a limited period of time. In addition, Skype Technologies S.A., periodically renews them to further enhance security.

At the point when a Skype client gets a signed digital credential and can validate its authenticity, the Skype client may (on behalf of a Skype user) present it to other Skype clients. When the authentication process is complete, there is no reason for the recipient to re-verify the authenticity of the caller's credential by checking in with the authentication server or any other piece of centralized infrastructure.

Note: To the Skype network, a Skype user is simply represented by a Skype name that has been authenticated properly to the network. Although a Skype user typically runs only one Skype client instance, an individual person can have multiple Skype accounts with unique Skype names, passwords, and profiles.

How are Skype Sessions Established?

When a Skype user wants to communicate with another Skype user, each connection and session are established uniquely.

While a Skype user is online, the user's Skype client maintains a persistent connection to a supernode. This enables presence on the Skype network; put simply, this is how one Skype client is able to constantly inform other Skype clients of the user's availability and on-line status.

Moreover, when a Skype user attempts to communicate with others, the caller's Skype client checks with the global index—the distributed database of users that is maintained in the hierarchy of supernodes—to see whether the intended recipient is, in fact, online, regardless of how the recipient has set his or her on-line status.

Note: For brevity, the following sequence will not distinguish between voice / video calls, instant messages (IMs), and file transfers. It will simply refer to a caller and recipient to keep things simple.

If the intended recipient is online, the caller's Skype client collects both the recipient's Skype client's network address and the network address for the recipient's Skype client's supernode from the global index.

Next, the caller's Skype client attempts to make a direct connection to the recipient's Skype client. Assuming the Skype clients can connect directly to one another, communication begins.

It is not always possible to establish a direct connection right away. This can happen, for example, when a recipient's Skype client is behind a firewall or NAT device. So, by design, if the first attempt at a direction connection fails, the caller's Skype client transmits a message to the intended recipient's client by way of supernodes.

The message that Skype transmits is intended to alert the recipient's Skype client of two things: first, the caller's Skype client wants to connect, and second, it can't connect directly. The message also asks the recipient's Skype client to try to establish a direct connection in the opposite direction; in effect saying, "I can't reach you directly, can you reach me?"

If the Skype client can establish a direct connection using the reverse communication path, then communication begins. The message content is transmitted directly from one Skype client to the other.

However, if there is no way for the Skype clients to communicate directly with one another, Skype will attempt to route the content of the communication through a relay host, which is another kind of special node on the Skype network. Relay hosts are similar to supernodes because they are regular Skype peer nodes that, under a particular set of circumstances, take on additional responsibilities.

They are responsible for detecting Skype clients which are online, establishing connections among them, and transmitting signaling messages to ensure encrypted traffic is routed efficiently.

A relay host is similar to a supernode but, instead of operating as a temporary directory index server for nearby peer nodes in the cluster, a relay host is not actually party to the call. Instead, relay hosts simply provide an alternative path for Skype network traffic. In other words, they are data-transfer stations that offer a clear path to connects Skype clients which are unable to connect directly.

When this happens, both the caller's and recipient's Skype clients connect to the relay host. In truth, the Skype network traffic is spread among multiple relay hosts for fault tolerance, as well as to ensure call quality and call completion. And all of the relay hosts remain "in play" for the duration of a specific session. They are dismissed when the communication is complete.

To restate what has already been said, the reason that Skype transport-layer security is essential in the Skype P2P architecture is that in order to complete a connection, supernodes are always (and relay hosts may sometimes be) involved in communication among Skype clients. The Skype security model prevents eavesdropping because all communication between each pair of nodes, supernodes, and relay hosts is encrypted end to end.

How Is Encryption Handled?

Skype relies on a system of public and private keys to ensure the contents of communication are confidential. As stated earlier, all Skype network traffic is encrypted to ensure privacy. This includes all signals used to control the Skype network, as well as communications content; specifically, voice video, text, and data.

The use of strong encryption here means that it is not possible to know what information is traveling in the Skype network among nodes, supernodes, or relay hosts.

The cryptographic model behind Skype employs both public-key and symmetric-key cryptography, including the AES algorithm, used in 256- bit integer counter mode. Skype also uses 1,024-bit RSA to negotiate symmetric AES keys. User public keys are certified by the Skype server at login, using 1,536- or 2,048-bit RSA certificates.

At the moment the Skype clients establish a connection (but before an actual voice or video call, text chat, or file transfer begins), each Skype client involved in the session presents digital credential and must agree on an Advanced Encryption Standard (AES) encryption key.

Each Skype client generates half of a 256-bit symmetric key when a connection is established. The keys are exchanged and joined to create a 256-bit session key, which is valid for the life of the session. Every session gets an individual 256-bit key. In the case of a multi-party conference call, multiple simultaneous calls are set up, each with its own session and unique key. The fact that symmetric AES keys are shared enables Skype to be an authenticated channel between any number of valid Skype users.

Note: AES has been adopted by the United States government to protect sensitive information. With 256-bit encryption, any of 1.1 x 1,077 possible keys may encrypt sensitive data.

Skype relies on public-key cryptography to validate signatures on credentials for the purpose of negotiating a symmetric key, then it uses symmetric-key cryptography for secure communication between Skype clients. The combined approach makes the process of establishing transport-layer security among Skype clients efficient.

The public-key cryptographic model enables two things. It permits a Skype client to receive private messages which only it can read, and it lets the Skype client issue signed messages that no one else could have created. No person, organization, nor Skype Technologies S.A., itself has a copy of a key being shared by the parties to a Skype call.

Moreover, there is no sharing or disclosure of keys to any parties other than the pairwise sharing to establish a 256-bit session key. Finally, when a Skype session ends, the keys are discarded. And encryption keys are not disclosed to the Skype user or escrowed to third parties.

Security & File Transfers (Viruses, Trojan Horses, etc.)

A particularly powerful feature of Skype is its capability to enable users to transfer files securely between computers.

On the Microsoft Windows platform, system- and network administrators can turn off the Skype client's file transfer capability by setting a registry key. See Setting Policies via Registry Keys later in this document.

The Skype file transfer capability allows a Skype user to send files of up to 2GB to anybody in their contacts list. The intended recipient must meet the following four criteria:

- Has shared contact details (see "Privacy and Sharing Contact Details),
- Has not blocked the sender (see "Blocking Other Skype Users"),
- Is online when the sender initiates the file transfer, and
- Is willing and able to accept the file transfer from the sender.

Note: Sometimes, a Skype user will appear online but, in fact, will not be notified of a pending file transfer until the intended recipient receives some type of initial contact, such as an IM or call, to re-establish the connection between Skype clients.

The Skype client maintains a history of each user's file transfers, those that are sent and received. This list is displayed in the history tab, unless the user clears the list intentionally. The list also shows the origin or destination on the file system of the transferred file.

While Skype's file-transfer capability provides a convenient and secure channel for sending and receiving digital files, along with this newfound capability, comes the risk of inadvertently downloading a file that contains a virus, Trojan horse, or spyware.

So, in much the same way that enterprise users must be thoughtful about opening email attachments or downloading files from the Internet, users must take special precautions when accepting file transfers from other Skype users.

Anti-Virus Shields and Real-time Scanning

All major antivirus software vendors provide anti-virus "shield" capabilities which should be configured to perform real-time scanning. As you recall, all Skype network traffic is encrypted end to end. The Skype client decrypts incoming file transfers only when the user accepts to receive them.

In real-time, as Skype decrypts each file, the anti-virus software on a Skype user's computer will scan it. Therefore, if people in your organization are using or intend to use Skype, it is important to:

- Configure anti-virus software to scan *all* incoming files,
- Be vigilant about keeping anti-virus definitions up to date, or
- Turn off the file transfer capability as described later in this document.

Doing these things will prevent your Skype users from inadvertently saving an potentially infected file to the file system (that is, as long as an anti-virus product is running, the virus or Trojan horse is known).

Note: The current version of Skype does not yet support centralized anti-virus scanning.

When any software program wishes to read from or write to a file on disk, the application wishing to access the file calls the open() primitive from the kernel to attempt the appropriate access, as is shown in the left panel. When Skype, for instance, reads a file the user wishes to transmit, or when Skype writes the file on the receiving end, the Skype client requests to create, open, read from or write to the file as appropriate.

Antivirus tools make use of the fact that all file access is done through a small number of kernel primitives by employing one of several techniques, depending on the type of operating system in use, to "shim", wrap or intercept all calls to all file access kernel functions.

Therefore, if a user attempts to use Skype to send or receive a file, the antivirus program will detect the attempt to read or write a file containing and deny the Skype client the permission to continue writing.

As is shown in the right-hand panel of figure 6, the antivirus (AV) program inserts itself in the file access chain, which gives it the opportunity to watch for file contents which match known virus signatures.

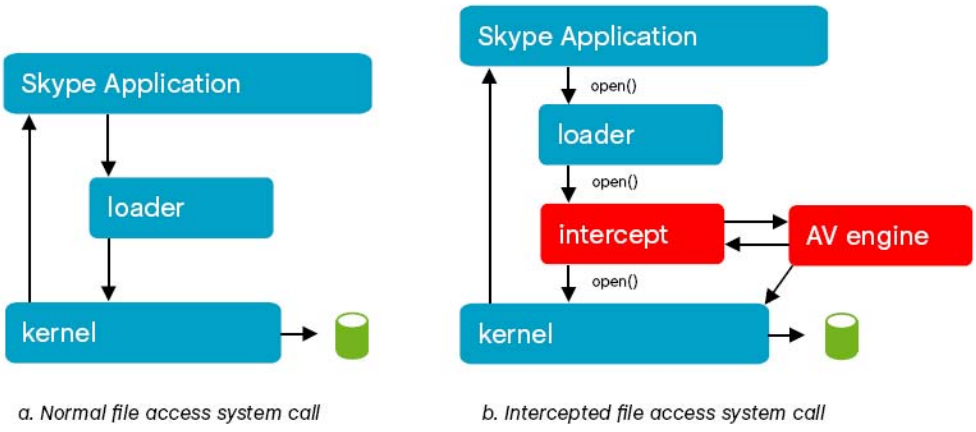

Figure 3. Real-time Anti-Virus Scanning of File Transfers

To illustrate this point, we sent an industry-standard virus scanner test file, called the EICAR test file, from an unprotected computer to a Skype user on a Microsoft Windows XP computer that was protected with a retail copy of Norton AntiVirus Professional.

Although the Skype client would have otherwise allowed the file transfer, the file was immediately caught and deleted by Norton AntiVirus, while the user was alerted by the Norton popup dialog box shown in Figure 7.

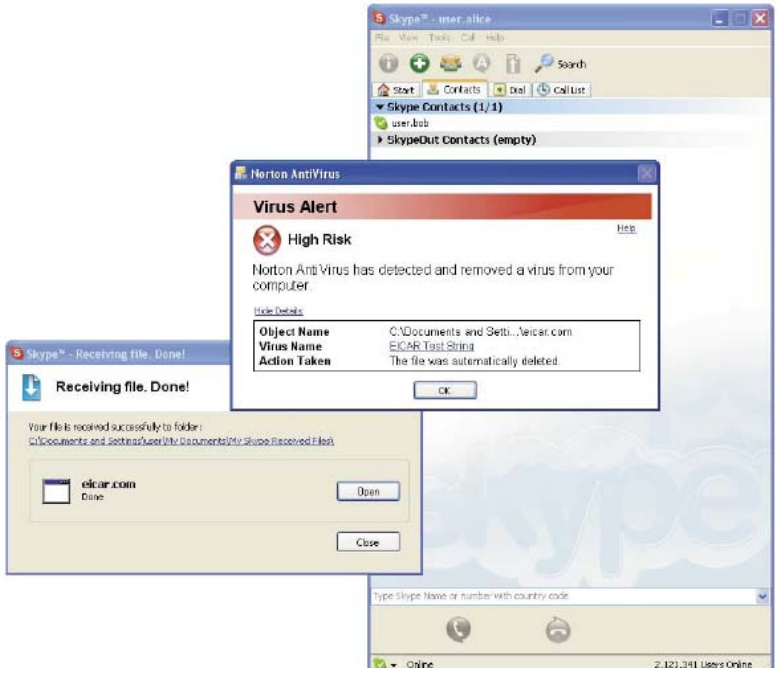

Figure 4. Norton AntiVirus stopping the EICAR antivirus test file over Skype

Privacy and Sharing Contact Details

To help manage communication and protect privacy, the Skype client supports a set of features to give users control of who can see their on-line status (presence information) and who can contact them. In earlier versions of Skype, this system was referred to as *authorizations*.

In general, sharing contact details issues an approval certificate that one Skype user transmits to another Skype user to grant permission to see on-line status. Sharing contact details also gives the user permission to communicate freely (call, send IMs, etc.) by avoiding restrictions that apply to other, non-authorized users, depending on how a given Skype user has configured his or her privacy preference settings.

Each time a Skype user adds a Skype name to his Contacts List, the Skype client prompts that user to send a request to share contact details. If the intended person grants the request, both users will be able to see each other's on-line status. See "An Example – Sharing Contact Details" to see how this process unfolds.

If the user denies or ignores the request, his on-line status information will not be visible to the person who sent the request.

If a user adds a Skype name to his contact list but is not granted permission, the on-line status information associated with the Skype name is not displayed, and the user gains no special privileges to communicate with the Skype name based on privacy preferences set by the user.

A request to share contact details involves a digital signature that gets assigned to the request, which (once signed) is then sent back to the requestor. It is tied to the same sign-in credential that is used to authenticate a Skype identity. This method does not simply set flag or a bit in the message. Therefore, is nearly impossible to fool the system.

Without a doubt, the ability to share contact details is important for Skype users to be able to maintain their privacy. It is also essential for maintaining control of who can contact users. Skype allows each user to set his or her own privacy thresholds in terms of who can call and send IMs.

Specifically, Skype users can set voice/video calling preferences which allow them to specify that:

- Anyone can call,
- Only people on a user's Contacts List can call, and
- Only people who are authorized can call.

Users can set IM preferences independently to specify that:

- Anyone can send an IM,
- Only people on the user's Contacts List can IM,
- Only people the user has authorized can send an IM, and
- File-transfer preferences can be set independently of both calls and IMs.

An Example - Sharing Contact Details

Every time a user adds another user to his or her contact list, a request to share contact details is generated.

For example, lets say that user Bob wishes to add user Alice to his contact list. In this case, Bob would select Tools ->Add a Contact... and enter Alice as the Skype username to add to his contact list.

Bob would immediately be presented with a window labeled "Say Hello…", which includes a blank text-input box to give Bob an opportunity to Alice who he is and why he is wants to share contact details. This introduction text is particularly helpful if Alice was not expecting Bob's request.

When Bob completes the message text and clicks OK, the request will be sent from Bob directly to Alice.

Because Alice has not yet shared her contact details with Bob, Bob cannot see Alice's on-line status. In addition, if Alice is not logged in to Skype when Bob sends the initial request, the request will actually be sent the next time both Bob and Alice are logged on at the same time.

Eventually, Alice will receive Bob's request message in a special window that is clearly labeled as an incoming request for her to share her contact details. Alice gets to choose how she wants to handle the request. She can accept Bobs request. Or she can reject it.

If Alice decides to accept Bob's request, then she would choose to "allow this user to see when I'm online" and click OK. If, on the other hand, she rejects Bob's request, she would select the "do not allow this user to see when I'm online".

In either case, once Alice makes her decision, her answer is returned to Bob's Skype client. And, if she approved the request, then the message that is sent to Bob's Skype client would immediately begin to display Alice's on-line status.

Here we show an unwanted request sent by Skype user Charlie to user Alice. As usual, Charlie created the request by adding Alice to his contact list. But, in this case, Alice decided not to share her contact details and disclose her on-line status to Charlie.

In effect, Alice rejected Charlie's request. Although a denial message is returned to Charlie's Skype client to close out the request, Charlie will not be informed of the "rejection". In other words, from Charlie's perspective, Alice's on-line status simply remains a question mark.

Blocking Other Skype Users

To give Skype users control over who contacts them, Skype supports the ability to block another Skype user, even if contact details have already been shared.

Blocking a Skype user does two things: it stops the Skype user who has been blocked from communicating with the user who has performed the blocking, and from seeing his or her on-line status.

If a user *un*blocks a Skype user, do the users need to share contact details again? No, for all intents and purposes, sharing contact details is permanent. Once a request is sent to another user, there is no way to take it back. However, blocking can be used effectively to nullify a request to share contact details.

The Skype client allows users to create and manage a list of blocked users through the privacy preferences, as well as by selecting Tools ->Manage Blocked Users. Once a Skype name is added to this list (and until it is removed) a Skype user who is blocked will be unable to see the on-line status and cannot initiate contact via Skype.

Users who have been blocked may be unblocked at any time by the user who put the block in place, simply by removing the blocked user's name from the blocking list.

Preventing "spam" and "spit"

Spam is the scourge of today's Internet. Unsolicited commercial e-mail is an unwanted reality of e-mail communications today. Skype has taken steps to prevent the use of Skype as a tool to help spammers or those who spam over internet telephony ("spit").

Users can take an active role in countering spam and spit by authorizing only users whose identity they have confirmed. Users can set their privacy settings to that they can be called only by persons who know them. Users can include a note in their Skype Profile asking potential callers to send them a chat message before calling.

In addition, Skype does not make e-mail addresses available to people who might try to use the Skype on-line directory to find potential advertising targets. Even though Skype users may include their e-mail address in their Skype profile, email addresses are not be made available to others.

Note: A valid email address in a user's Skype profile enables lost password recovery and allows other Skype users to use the email address as a search term when adding Skype names to their contact lists. Refer to "Where Does Skype Store Data" below for more information on how Skype handles email addresses.

Just as is the case with any e-mail and/or web communication, Skype users should know they are communicating with before they divulge any private information over Skype.

As described earlier, Skype's security model ensures that no one can counterfeit a user's Skype identity or easily masquerade as someone else. But like email, it is each Skype user's responsibility to prevent their Skype account from being accessible by persons other than themselves, especially in situations where other people may have access to or be sharing the same computer. Please report abuse to Skype by e-mail to abuse@skype.net.

How to Prevent Phishing

Skype will never, under any circumstances, ask Skype users to divulge passwords over email.

As is the case in other e-commerce sectors of the Internet, Skype users might receive false e-mails or encounter third-party web pages designed to look like e-mails or web pages created by Skype Technologies S.A., and intended to con users into giving up their Skype name and password. This kind of attempt to collect user's credentials has been given the name "phishing", and it is rapidly becoming the #1 threat to individual users on the Internet.

Inform users that they should use their Skype user password only for logging into the Skype client itself, when managing their Skype account on the web at https://secure.skype.com/store/member/login.html, or logging into other know-to-be-valid Skype accounts such as https://developer.skype.com and https://skypecasts.skype.com.

If a Skype user believes he has been the victim of phishing, he should change his password immediately and refer the situation to Skype Abuse by e-mail to abuse@skype.net. IT administrator's can help by describing these types of problems in detail and include any phishing e-mails or URLs of the phisher's web page.

Where Does Skype Store Data?

Skype maintains information about users in the following locations: the Skype central authentication server, Skype account and transaction servers, a Skype event server, the global index in the Skype P2P network cloud on the Internet, a Skype users' computer, and other Skype users' computers.

- A Skype user's computer stores the installed version of the Skype client, any residual copies of Skype installation files that have not been deleted, Windows registry keys, profile information (including email address), voicemail message files that have been delivered, call logs, chat logs, and a set of configuration files that may include the Skype names of people in a given user's contacts list. Chat logs are saved indefinitely in hidden directory under the user's home directory by default unless a user intentionally deletes them. The Skype client can be configured to delete or expire.

Important note: Trace bits of information related to one Skype user might be found on another Skype user's computer. This type of information may include voicemail messages that have been received or not yet been sent, IM's that have not been sent and/or chat histories.

- The Skype central authentication server stores data about all valid Skype users. This database does not accept queries from any non-Skype source. Specifically, it stores Skype name, a copy of the e-mail address that was originally provided during registration, and a one-way encrypted hash of each user's password.

  Skype maintains two references to each user's email address, one is in the profile on the Skype user's computer. The other is stored in My Account on the Skype website for password recovery. As a result, if the email address changes, it should be updated in both the user's Skype client profile *and* the Skype website.

- Skype account / transaction servers capture statistics about Skype calls as well as order and transaction data for the purpose of operating the Skype service.

  Skype-to-Skype traffic data is collected only in the aggregate. Skype Technologies S.A., does not track information about which users are communicating with one another over the Skype network or the duration of these interactions. However, information about SkypeIn and SkypeOut calls is collected and processed to manage the business. If a user has SkypeOut credit, information about the calls they place is collected to maintained in their account balance. For a detailed explanation of how this data are used, please refer to the Skype Terms of Service, which is available on the Skype Web site.

- The Skype event server is a database that Skype utilizes as a cache to store temporarily a copy of certain types of information until the information is no longer needed; in other words, to ensure that the information is delivered reliably. In general, Skype Technologies S.A., does not maintain copies of information.

- The global index stores each user's computer's last network address, the network address, each Skype client's supernode, and each user's current Skype user profile. All profile data in the public directory is digitally signed.

Files, Folders, & Application Data Locations

When this process runs:	The following directory, file, or registry key is created:
Skype installer (SkypeSetup.exe)	1. If the installing account has Administrator privileges, the Skype shared program is written to the %programfiles%directory, which is usually C:\Program Files\Skype\Phone\ 2. If the installing account has limited privileges, the Skype program is written in the %homedrive%:\%homepath%directory, usually C:\Documents and Settings\<username>\Application Data\Skype\ 3. Several folders with names beginning with "My Skype", such as My Skype Pictures (which contains common icons used by the Skype client) are created in the %allusersprofile% directory, which is usually C:\Documents and Settings\All Users\Documents\My Skype Pictures\. 4. A temporary folder is created in the user's %temp% directory for the purpose of expanding the installation executables during the setup process. This directory and its contents are deleted after the setup process concludes. 5. Several default file locations are stored in a persistent way in the Windows registry under the following registry key: HKLM\SOFTWARE\Skype 6. Some other registry keys may be created by other Windows subsystems as a consequence of Skype registering its installation on the platform, for instance: - Registration of the callto:// URL handler - Obtaining Windows Firewall inbound connection approval
Skype (client) application	1. A Skype folder is created for the individual user which may be used to store user-specific information. This folder is usually C:\Documents and Settings\<username>\Documents\Skype\. 2. A folder named My Skype Pictures may be created in the user's Skype folder, which is usually C:\Documents and Settings\<username>\Documents\My Skype Pictures\. This folder contains any icons which may be created or used by an individual and which is not common to all users on the platform. 3. If not created during the installation process, a folder named Skype may be created in the user's Application Data directory. This directory stores ephemeral information pertaining to a user's Skype sessions. This folder is usually C:\Documents and Settings\<username>\Local Settings\Application Data\Skype\.

Passwords

As discussed earlier, Skype Technologies S.A., never, under any circumstances, requests a user's Skype account name or password by e-mail.

Skype passwords are stored as one-way encrypted hash and should remain completely secret.

Currently, the only places Skype requires a password are for:

- Logging into the Skype client itself,
- Managing users' Skype account on the web at https://secure.skype.com/store/member/login.html,
- Logging into other know-to-be-valid Skype accounts such as https://developer.skype.com or https://skypecasts.skype.com.

If a user wants to create a new password, he or she can go to the account page on the Skype Web site as long as an e-mail address was provided during registration and that address is still valid.

Important: Skype maintains two references to each user's email address, one is in the profile on the Skype user's computer. The other is stored in "My Account" on the Skype website for password recovery. As a result, if the email address changes, it should be updated in both the user's Skype client profile and the Skype website.

Adware and Spyware

Neither the Skype client nor the Skype installation program include any adware or spyware.

However, it is possible to find seemingly legitimate installers on the Internet that, without appropriate permission, have bundled the Skype client improperly with third-party software which very well might include adware or spyware.

Therefore, we *strongly* recommend that you get the most current version of Skype by downloading it from the Skype Web site at www.skype.com/download.

In addition, Skype software installers for Microsoft Windows XP, Windows 2000, and Windows Pocket PC 2003, as well as the Skype application itself, are digitally signed.

This enables you to verify the Skype software installer's digital signature before you install the Skype client on any of your systems, which prevents you from accidentally installing any spyware or malware when you install Skype on your network.

In addition, although technically you can perform the digital signature verification test on the Skype client after the installer has been run, we recommend that you verify the authenticity of Skype installer *before* you install the Skype client.

For a detailed explanation of how to perform the digital signature verification test, refer "Deploying Skype In the Enterprise" later in this document.

Skype Security Evaluation

Skype.com contains resources for network administrators and more detailed information on Skype security. Go to www.skype.com/security for specific security-related information including Skype Security Bulletins, contact email addresses, and PGP keys for verifying digital signatures.

This link also includes Skype security evaluation report by Tom Berson of Anagram Laboratories. This report presents:

- An in-depth review of the security framework that is incorporated into Skype products
- A description of the protective mechanisms that are in use throughout the Skype infrastructure
- The general security policy that defines the basis for all designs within Skype's operational framework

Skype Security FAQ

Increasingly, companies are leveraging the benefits of Skype to enhance customer support activities by:

- Enabling customers to contact the company's call center via the Skype client,
- Utilizing Skype's Call Forwarding capability, and
- Forwarding calls to a PSTN number ending at your company's call center switch.

While Skype was originally designed as a consumer application that offers a private communication channel among Skype users, as enterprises incorporate Skype into their mission-critical operations, certain questions about security of customer communications naturally arise.

Here are some of these questions and their respective answers:

Is "Hole Punching" a Security Issue?

No. One of the difficulties that plagues many VoIP solutions is that the call is unable to pass across network boundaries. This problem may arise due to the presence of network address translation (NAT) equipment at the network's boundary, or the result of restrictive rules put in place on a firewall at the network edge.

To allow users the greatest possible flexibility, Skype has implemented a robust set of NAT traversal techniques in its software, allowing Skype frequently to be able to operate in situations where traditional VoIP telephony would fail.

It is common in most home and office networks today to use network address translation to allow easier administration of the network without requiring each network to obtain its own block of scarce network addresses.

An effective way to set up P2P communications between two computers hosted on private networks—ones behind NAT devices—is to use a technique called "hole punching". This technique is widely used by application software communicating using UDP packets and can also be used to establish connections using the more reliable TCP protocol.

Although the name "hole punching" might suggest otherwise, this technique does not compromise the security of private networks but instead seeks to establish communications by working within the policy framework of most NATs. These techniques signal to the NAT devices in the path of a communication that the P2P sessions have been solicited and should therefore be passed.

How Secure is the Skype telephony connection?

Can anybody listen in on customer phone calls? No.

Skype's security is integrally linked to its architecture. All voice calls, chat messages, video calls, and file transfers are encrypted end-to-end (in the Skype network) to ensure privacy.

Even though Skype does not guarantee complete anonymity or secrecy, it does provide industry-leading transport layer security to ensure that message content traveling over the Skype network on the Internet cannot be tapped or intercepted.

To accomplish this, Skype relies on a system of public and private keys to keep the contents of communication confidential. This includes all signals used to control the Skype network as well as communications content such as voice, video, text, and data. The use of encryption means it is not possible to know what information is traveling in the Skype network among integral parts, including nodes, supernodes or relay hosts.

Skype's network traffic cannot be intercepted and decoded while in transit. The cryptographic model behind Skype employs both public key and symmetric key cryptography, including the AES algorithm, used in 256-bit integer counter mode. Skype also uses 1024-bit RSA to negotiate symmetric AES keys. User public keys are certified by the Skype server at login using 1536 or 2048-bit RSA certificates.

All communications between any pair of Skye users is sent simultaneously over a single session, using a technique called multiplexing. The contents of voice calls, text chats and any other form of Skype communication is sent with an equal degree of security.

However, while Skype does offer a private communication channel, network administrators must keep in mind that Skype runs on mass-market operating systems. This means that Skype provides an operational level of security or privacy for Skype users in the context of the security provided by Microsoft Windows, Mac OS X, Pocket PC, Linux, and the other operating systems on which the Skype application runs.

Therefore, Skype does not provide a secure communication platform in the strictest sense, and it is not a secure file storage solution either. As a result, Skype-related data, transmissions, and files are only as secure as the data on the computing devices running the Skype client.

In other words, while Skype network traffic cannot be intercepted and decoded in transit, once it is decrypted the streaming audio/video, and audio/video/text files may be vulnerable to malicious attacks, depending on the level of security that the user has in effect.

Once a text message, file transfer, or audio/video stream is received by the intended receiver, the Skype client cannot prevent the copying, archiving or redistribution of the received message.

The bottom line is this. The Skype client protects the confidentiality communications while in transit, whether the connection is made directly between Skype clients or is relayed through a third party.

It remains the responsibility of users themselves to protect their communications prior to sending and, similarly, following receipt, just as they would with e-mail, and email attachments.

Is Call Forwarding to a PSTN less secure? Yes and no.

In the Skype network, all voice calls, chat messages, video calls, and file transfers are encrypted end-to-end to ensure privacy. However, at the point a Skype voice call leaves the Skype network, the call is decrypted:

- When a Skype voice call leaves the Skype network and enters a traditional telephony network through a termination provider, the call is decrypted and sent over the PSTN the way that any voice call may be transmitted over the PSTN. As a result, the call becomes susceptible to advanced techniques used by law enforcement and others to "tap the line".
- Similarly, when a Skype call leaves the Skype network and enters a call center through a SIP (Session Initiation Protocol) gateway, the Skype call is no longer under Skype's control and is unencrypted at that point forward.

Therefore, given a scenario whereby a customer or account holder uses Skype to contact the company, and whereby the call is forwarded to a PSTN number that terminates at the company's call center switch, you can consider calls that originate on Skype to have the same operational level of security and privacy as calls that originate and terminate over the PSTN or call center.

There is one caveat, however. As mentioned above, IT administrators must consider that Skype runs on mass-market operating systems. This means that Skype can only provide an operational level of security or privacy afforded to Skype users in the context of the security provided by the operating systems on which the Skype client runs.

Given this, even though Skype network traffic cannot be intercepted and decoded while in transit, audio files for voicemail messages and text files associated with chat histories may be vulnerable on end user computers and file systems, depending on the level of security present on the user's network and computer.

Are Skype Users at Risk of Trojan Viruses and Other Threats?

For obvious reasons, malicious code such as Trojan viruses, malware, adware, and spyware remain high on the list of concerns for IT management and security personnel. The question about whether end users are susceptible to such threats must be addressed in two separate ways.

Can a Hacker Send a Trojan Virus via Skype to an IVR? No.

Skype's capability to enable end users to send and receive files (which may include potentially malicious code) utilizes Skype's File Transfer feature, which lets a Skype user send a file to one or more other Skype users.

Such files cannot be transmitted surreptitiously via Skype's pseudo-isochronous voice or video stream so there is no risk of a hacker transmitting a Trojan virus (or other file) to either the company's IVR or the Skype user's computer.

Refer to "Enterprise-Wide Installation and Setting Policies" for information on how to disable this feature using a Group Policy Object or Registry Key.

Can a User Accept a Trojan Horse? Yes and No, It's just like email attachments.

Before a Skype user accepts a file transfer from another Skype user, the recipient should have up-to-date anti-virus software installed and configured to scan all incoming files, even from people who they know.

Skype's File Transfer feature gives Skype end users a convenient, secure channel for sharing photographs, documents and other electronic files with other people on the Skype network. Unfortunately, along with any newfound ability to share data comes the risk of inadvertently accepting a malicious file that contains a virus, Trojan horse, or spyware.

The good news is that Skype's File Transfer feature only works among instances of the Skype client. The Skype client enables a Skype user to request that another Skype user accept a file, which (upon acceptance) will be downloaded to the recipient's computer. Put simply, file transfers can only take place and with the explicit consent of each recipient.

As a result, in precisely the same way that every end user must be cautious when they accept an email attachment or download a file from the Internet, they will reduce the risk of infecting their computer if they think before they accept a file transfer, especially from people who they don't know.

Refer to the section above, entitled "Security & File Transfers" for more detailed information.

Deploying Skype in the Enterprise

First things first

Our goal is to enable users to enjoy Skype from as wide a variety of networks as possible, without requiring people to understand or configure complex options such as relay hosts or preferred network ports. In this sense, Skype is generally "hands-off ."

The authentic and most up-to-date version of Skype is always available directly from Skype's own download server at http://www.skype.net/download/. While we recommend that you obtain Skype directly from our servers, third parties are permitted to host downloads of Skype's application, provided they follow the terms in Skype's End User License Agreement (EULA) concerning redistribution of Skype software.

Once installed, the Skype client periodically checks to see if there is a software update available, although system- or network administrators may disable this feature. And end users can adjust their Skype client preferences to control how updates and patches are handled in general.

General Guidelines

Skype Technologies S.A., wants end users and enterprises alike to have a safe and enjoyable experience using Skype to enable communications. Toward this end, we would like to underscore the importance of keeping your company's computers and users safe and secure while doing so.

We have published our recommendations for general computer security on our main web site at http://www.skype.com/help/guides/staysecure.html. In addition, we would like to highlight some of the main points:

- Before you deploy Skype in an organization or redistribute it to others, be sure it is an authentic copy. Check the digital signature of the installer and be sure to follow the limitations in Skype's Terms of Service before redistributing Skype software.
- Keep your organization's computers up-to-date with relevant patches. Most of the computer security problems on the Internet today can be traced back to improperly patched computers.
- Obvious as it may sound, use anti-virus protection, even on non-Microsoft computers such as the Apple Macintosh, and keep the virus definitions constantly updated.
- When you use Skype, know who you're authorizing and don't hesitate to block users who are making unwanted contact. Keep user profiles up-to-date, but also know that everything in a user's profile (except e-mail addresses which are masked for privacy) are viewable to others whose search criteria matches the information in the profile.
- Always authenticate other parties before beginning to discuss any confidential business or sensitive personal information. Remember that although Skype takes care to protect communications from unwanted disclosure, there is the remote possible that your computer, or those belonging to persons with whom you are communicating have been "hacked" or compromised in some way.

- Instruct your users to choose good passwords for Skype and change them regularly. Remember, users should never check "remember my password" when using Skype on a shared computer.

How to Determine if your Network is Skype-Friendly?

In general, most firewalls, routers, and NAT devices are Skype-friendly. Typically they are configured to handle UDP traffic properly by default.

You can determine if your network is Skype friendly this with freeware called NAT Check, created by Bryan Ford. NAT Check lets you test your network to determine if the UDP traffic is handled properly; in other words, that UDP translation is compatible with a P2P protocol such as Skype. Downloadable NAT Check from http://midcomp2p.sourceforge.net.

Make sure that your network's UDP translation shows consistent translation. Also be certain that the input and output ports are identical (except in the event of a conflict loopback translation). And, make sure that unsolicited UDP packets that get sent to the network are filtered or discarded. Last but not least, Skype prefers that your network's firewall or NAT gateway supports IP packet fragmentation and reassembly. However, this is not a hard requirement.

Skype does require, however, that your firewall not block attempts to send parallel UDP packets or TCP connection attempts to multiple ports at the destination address. The reason? Some firewalls mistakenly classify this as port scanning and block the host as a result. This does not only affect Skype adversely, but also may adversely impact other legitimate network applications running on the same host computer.

Verifying the Authenticity of the Skype Installer for Windows

To ensure that you have the most current version of Skype, download it from the Skype Web site at www.skype.com/download.

It is possible to get Skype from third parties as well, in part because Skype Technologies S.A. allows third parties to host downloaded versions of the client; that is, as long as the third party in question adheres to the terms of Skype's End User License Agreement (EULA) regarding the redistribution of the Skype client.

Note: According to the terms of the Skype Terms of Service and EULA, third parties may not repackage or wrap the Skype application in any other software.

Skype software installers for Microsoft Windows XP, Windows 2000, and Windows Pocket PC 2003, as well as the Skype application itself, are digitally signed. So, to guarantee that you have an authentic version of the Skype, and to prevent accidentally installing any malware or spyware, you should verify the Skype software installer's digital signature before you install it.

You can perform the digital signature verification test on an installed Skype executable program once the Skype installer has been run, but it is best to verify the authenticity of the digital signature before Skype is installed and run.

Skype for Linux distributions that are packaged in rpm format are signed using Skype's signing key, which you can download from the Skype Web site at www.skype.com/products/skype/linux.

To verify installer authenticity for Microsoft Windows, follow these steps:

1. Locate the Skype installer program. Open the Windows File Explorer and navigating to the Skype installer program if necessary.

2. Right-click the Skype installer program. Then select Properties from the pop-up context menu. The Properties dialog box for the Skype installer is displayed.

3. One of the tabs at the top of the Properties dialog box should be labeled "Digital Signatures". If you do not see this tab, STOP. Then skip to the next section, "Problems with a Digital Signature". If you do see the Digital Signatures tab, continue to step 4.

4. In the Properties dialog box, a list of digital signatures that apply to this installer is displayed. You should see only one signer of the installer package: Skype Technologies SA. Double-click the line that contains Skype Technologies SA. This displays a window that contains the details of Skype's digital signature.

5. Verify that the pop-up window labeled Digital Signature Information indicates that this digital signature is OK. If the pop-up window indicates that the digital signature is not valid, stop, because there is a problem, and skip to the "Problems with a Digital Signature" section that follows. Otherwise, continue to step 6.

6. Next, click the View Certificate button to display the details of the digital certificate that was used to sign the installer software. The pop-up window labeled Certificate should show you this:

```
Issued to: Skype Technologies SA
Issued by: VeriSign Class 3 Code Signing 2001 CA
```

If the text in either of the fields in the pop-up window is different from what is shown above (except for the year of the signing because it changes every 12 months) STOP, because there is a problem with the installer's digital signature. Then skip to the "Problems with a Digital Signature" section that follows. However, if it is OK, continue to step 7.

7. Click the Details tab to display the serial number of the signing certificate. Verify the certificate serial number with the appropriate serial number, available from the Skype Security Web site at www.skype.com/security.

If the certificate serial number for your copy of the Skype installer does not exactly match the one you get from the Skype Web site, STOP, because there is a problem with the installer's digital signature. If this happens, skip to the "Problems with a Digital Signature".

9. If you encountered no problems with the digital signature verification process, you can safely install the Skype client.

Problems with a Digital Signature

There are any number of reasons an invalid digital signature can appear on downloaded files.

One possibility is that the installer may have been corrupted accidentally while it was being downloaded. Another potential reason is that Skype may have been bundled improperly with a third-party software without appropriate permission. Or, someone may have tampered with a copy of the software to incorporate spyware, adware, or malware, violating the terms of the Skype End User License Agreement.

If you discover a problem with a Skype digital signature, it is important that you:

- Do not run any copy of the Skype installer that has failed a verification test.
- Contact the Skype security team via e-mail at security@skype.net and provide specific details, including information such as where you obtained the Skype installer.
- Download a fresh copy of the Skype installer from the Skype Web site, and verify the authenticity of the new installer as described in the preceding section.

Skype Client Notifications for New Versions and Updates

Once the Skype application is installed, it periodically checks to see whether an update is available by default. The Skype client does not update itself. Instead, the Skype client notifies the user when a more recent copy or critical patch is available. This gives gives the user the option to upgrade.

Users may chose to disregard these upgrade notices. System- and network administrators may disable this feature to control software installation policies. See "Enterprise Installation and Setting Policies" below.

End users can control the Skype automatic update-notification feature by a Skype application preference (choose Tools > Options > Advanced).

Alternatively, users may manually check to see if the copy of Skype they are running is the most current version. There are two ways to accomplish this:

- A user may select Help > Check for Updates from the Skype main window. This will launch the user's default web browser and display a message indicating whether the installed version is up to date, or
- Without launching the Skype client, a user may open the Windows Control Panel and double-click on Add or Remove Programs. Then, the user can find the entry for Skype and click on the entry labeled, "Click here for support information." Follow the hyperlink on the line entitled, "Product Updates" which launches the default web browser and indicates whether the installed version is up-to-date.

Enterprise-wide Installation and Setting Policies

Skype recognizes the challenges that enterprises and other organizations face with respect to managing sophisticated IT environments, as well as the complexity related to managing all of the different software applications and hardware in use today.

Therefore, setting policies via Group Policy Objects and registry keys is now supported, and MSI package installation is forthcoming as well.

Our goal is to enable system- and network administrators by making it easier and by improving control over the enterprise-wide deployment and management of Skype.

Policies

The Skype client adheres to the precedence of managed settings in order of the following priority:

1. HKLM Registry Keys (highest precedence)
2. HKCU Registry Keys
3. shared and config.xml Skype client settings
4. Skype client user preferences and defaults (lowest precedence)

Windows Registry

The Skype client has end user interface controls and/or functions for many of the features over which an enterprise might want to control. Some of the more technical and network-related features and configuration options are only accessible via the registry.

This is because enterprises who require such functionality generally have systems in place for centrally managing users' registries, and registry access control to ensure that users can't circumvent such settings.

XML Configuration Files

In addition to the Windows Registry, the Skype client relies on an XML file-based setup. Administrators (and users with appropriate permissions) may open and edit these configuration files even while Skype is running.

There are two XML files - shared and private. The shared file is named shared.xml and the private file is called config.xml. Remember that XML file entries are case sensitive, so "Debug" and "debug" are different.

See "Files, Folders, and Windows Registry Keys" above for the specific location on the filesystem of these XML configuration files.

Note: Proper XML syntax and format (closing, opening tags, etc.) is required. Otherwise, changes will not apply or the configuration will be lost if Skype is not running.

Setting Up Group Policies

As of Release 3.0, Skype now supports the use of Group Policies to deliver and apply desired policy settings and/or configurations to a set of enterprise users and computers within a Windows Active Directory environment.

The user of Group Policies provides system- and network administrators with the most convenient and reliable way to support centralized management of policy settings for Skype clients across an enterprise.

Skype policy settings set the behavior of the Skype client for a given set of targeted users or computers. Skype has been policy-enabled meaning that the behavior of the Skype client is determined and changes based on registry values indicated in an administrative template (`.adm`) file. This way, you can manage Skype's features and settings through registry-based policy.

Skype Technologies S.A., delivers these policy settings through a single Administrative Template file called `Skype-v1.5.adm`, which was designed to modify specific keys in the registry as described in the following section.

Note: You can download `Skype-v1.5.adm` from the Security section of the Skype website (Skype.com/security) to configure Skype policies using Group Policy Editor.

Registry-based policy settings appear and may be configured in the Group Policy Object Editor, which is under the Administrative Templates node.

The Skype-v1.5.adm file does not actually apply policy settings. Instead, it simply enables you to see the policy settings in the Group Policy Object Editor. From there, you can create Group Policy objects (GPOs) that contain the policy settings which you want.

For more information on how to deliver and apply group policies, refer to:

- **Open Group Policy as an MMC snap-in**
  http://technet2.microsoft.com/WindowsServer/en/library/ae13960b-3a27-4b19-a866-ed6e6e7a312d1033.mspx?mfr=true

- **Using Administrative Template Files with Registry-Based Group Policy**
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/gp/admtgp.mspx (See "Loading an .Adm File into the Group Policy Snap-in").

Configurable Policies

Following is the list of configurable policies that apply to the Skype 3.0 beta client:

Skype Client Functionality	
`DisableFileTransferPolicy`	Disable file transfer to prevent the user from sending and receiving files using Skype.
`DisableContactImportPolicy`	Disable import contacts.
`DisablePersonalisePolicy`	Disable personalization to prevent the user from changing sounds.
`DisableLanguageEditPolicy`	Disable language edit to prevent the user from editing language strings.
`WebStatusPolicy`	When enabled, always publishes the user's status on the web as Skype buttons, when disabled, prevents the user from publishing status on the web.

Skype Non-functional Capabilities	
DisableApiPolicy	Disable Skype Public API to prevent third-party applications from accessing Skype functionality.
DisableVersionCheckPolicy	Disable new version checking by preventing Skype from detecting new versions and updates.
MemoryOnlyPolicy	Run in memory-only mode so Skype does not store any data on the local disk.
Network-related Functionality	
ListenPortPolicy	Set the listening port where Skype listens for incoming connections.
ListenPort	Listening port number.
ListenHTTPPortsPolicy	When enabled, listen on HTTP (port 80) and HTTPS (port 443) ports; when disabled, don't listen on HTTP/HTTPS ports; when not configured, let the user decide.
DisableTCPListenPolicy	Disable listening for TCP connections to prevent the Skype client from receiving incoming TCP connections.
DisableUDPPolicy	Disable UDP communications to prevent the Skype client from using UDP to communicate with the network.
DisableSupernodePolicy	Prevent the Skype client to become a supernode.
ProxyPolicy	Establish the proxy policy.
ProxyType	Establish the proxy type.
ProxyUnset	Unset
ProxyAutomatic	Automatic
ProxyDisabled	Disabled
ProxyUnset	Unset
ProxyHTTPS	HTTPS
ProxySOCKS5	SOCKS5
ProxyAddress	Proxy address (host:port)
ProxyUsername	Username
ProxyPassword	Password

Registry Keys

Following is the list of registry keys that apply to the Skype 3.0 beta client:

HKEY_LOCAL_MACHINE (HKLM)

The registry keys for the local machine take precedence over the registry keys for the local user if there is a conflict.

```
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, DisableApi, REG_DWORD = {0,1}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, DisableFileTransfer, REG_DWORD = {0,1}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, MemoryOnly, REG_DWORD = {0,1}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, DisableContactImport, REG_DWORD = {0,1}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, DisableVersionCheck, REG_DWORD = {0,1}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, DisablePersonalise, REG_DWORD = {0,1}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, DisableLanguageEdit, REG_DWORD = {0,1}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, ListenPort, REG_DWORD = {0,1}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, ListenHTTPPorts, REG_DWORD = {0,1}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, DisableTCPListen, REG_DWORD = {0,1}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, DisableUDP, REG_DWORD = {0,1}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, DisableSupernode, REG_DWORD = {0,1}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, ProxySetting, REG_SZ = {string}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, ProxyAddress, REG_SZ = {string}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, ProxyUsername, REG_SZ = {string}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, ProxyPassword, REG_SZ = {string}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, WebStatus, REG_DWORD = {0,1}
```

HKEY_CURRENT_USER (HKCU)

The registry keys for the current user take precedence over the configuration parameters in the XML configuration files if there is a conflict.

The configuration parameters defined in the XML configuration files shared.xml and config.xml take precedence over any preferences the user selects in the Skype client if there is a conflict.

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableApi, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableFileTransfer, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, MemoryOnly, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableContactImport, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableVersionCheck, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisablePersonalise, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableLanguageEdit, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ListenPort, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ListenHTTPPorts, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableTCPListen, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableUDP, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableSupernode, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ProxySetting, REG_SZ = {string}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ProxyAddress, REG_SZ = {string}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ProxyUsername, REG_SZ = {string}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ProxyPassword, REG_SZ = {string}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, WebStatus, REG_DWORD = {0,1}