# Citrix Online Web Conferencing Tools: Security White Paper

Citrix Online provides true end-to-end data security measures that address both passive and active attacks against confidentiality, integrity and availability when using GoToMeeting, GoToWebinar and GoToTraining.

# Introduction

Citrix Online's GoToMeeting®, GoToWebinar® and GoToTraining™ tools are the most secure Web conferencing products available. For each solution, standards-based cryptography with true end-to-end encryption, a high availability hosted service infrastructure and an intuitive user interface combine to maximize confidentiality, integrity, and availability.

This document provides a technical description of the security features built into GoToMeeting, GoToWebinar and GoToTraining. It has been written for technical evaluators and security specialists who are responsible for ensuring the safety of their company's network and the privacy and integrity of business communications.

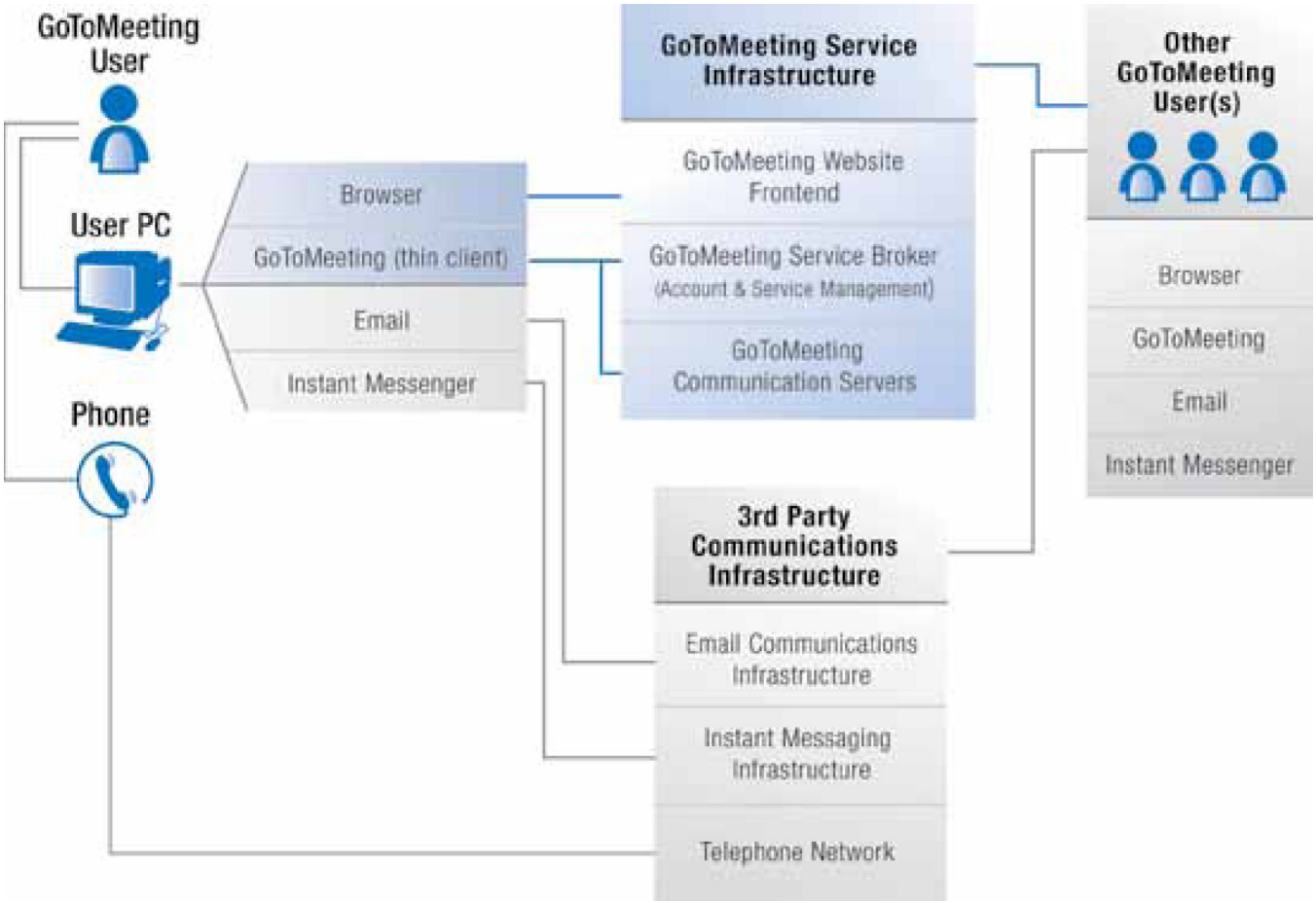


Figure 1

GoToMeeting, GoToWebinar and GoToTraining are Web conferencing tools that allow multiple PC and Mac users to interact using desktop screen sharing, remote keyboard/mouse control, text chat and other features. GoToMeeting is ideal for sales demos and collaborative online meetings; built for larger audiences, GoToWebinar is great for marketing presentations and company events; and GoToTraining provides features specifically for Web-based training, such as online access to tests and materials and a hosted course catalog.

These products are hosted services, delivered via Web browsers, downloadable client executables and a network of multicast communication servers operated by Citrix Online. Sessions are scheduled, convened and moderated using the Citrix Online Web site and client software. GoToMeeting, GoToWebinar and GoTraining automatically integrate with VoIP and phone conferencing for ease of use and solution completeness.

## Business needs for secure collaboration

Easy-to-use online business collaboration tools like GoToMeeting, GoToWebinar and GoToTraining can help companies increase productivity by enabling them to communicate and interact more effectively with co-workers, business partners and customers. But such tools vary greatly when it comes to embedded security features. Moreover, it is essential to understand the security implications of online collaboration and comply with safe usage guidelines.

Using any Web conferencing solution requires careful consideration of potential threats and resulting business risks. Business security needs that must typically be addressed when adopting a Web conferencing product include:

- Preventing unauthorized use of the service and its features so that only legitimate users and invited participants can schedule and participate in online sessions
- Avoiding any compromise of company assets, including client computers and the private networks to which they are attached
- Protecting the privacy and integrity of confidential communication, including screen sharing, text messages, email and voice interaction
- Ensuring availability and reliability of the service itself, so that business communications cannot be denied or disrupted
- Integrating seamlessly with other network/computer security measures, so that Web conferencing services can leverage (not degrade) an organization's existing safeguards

Our Web conferencing tools were developed from the ground up to satisfy these common business security needs. By incorporating security features and making them easy to administer and use, GoToMeeting, GoToWebinar and GoToTraining enable effective and safe online business collaboration.

## Role-based security features

To enable account owners to enforce company access policies related to service and feature use, every GoToMeeting, GoToWebinar and GoToTraining user is assigned one of several application-defined roles.

- Organizers are authorized to schedule meetings, Webinars and/or training sessions. An Organizer sets up each session, invites other users to participate, initiates and ends the session, and designates the current Presenter.
- Attendees are authorized to participate in sessions. Attendees can view the Presenter's screen, chat with other Attendees or view the Attendee list.

- Presenters are Attendees who are able to share their computer screens with other Attendees. Presenters also decide which other Attendees, if any, are permitted to control the keyboard and mouse of the Presenters' computers.
- Internal Administrators are Citrix Online staff members authorized to manage GoToMeeting, GoToWebinar and GoToTraining services and accounts
- External Administrators are individuals from a customer site authorized to manage multi-user accounts. External Administrators can configure account features, authorize Organizers and access a variety of reporting tools.

The GoToMeeting, GoToWebinar and GoToTraining user interfaces provide intuitive session controls and status indicators that facilitate productive and safe online sessions.

Controls and privileges available to each user depend on the currently assigned role: Organizer, active Presenter, or general Attendee.

## Organizer privileges

Organizers have the most control in a session and the ability to grant and revoke various privileges for the other participants.

Specific Organizer privileges include:

- The ability to invite Attendees, before or during the session, so that only authorized participants can join a given session
- The ability to see the complete list of Attendees and their current roles and privileges, so the Organizer remains aware of those present at all times
- The ability to start and end the session, which prevents others from disrupting the session accidentally or otherwise
- The ability to make any Attendee the active Presenter, controlling which desktop can be viewed at any point in time throughout the session
- The ability to disallow the use of Chat by one or more Attendees, and permitting "sidebar" discussions only when appropriate
- The ability to disconnect Attendees
- The ability to transfer the Organizer role to another Attendee so the session can continue if the Organizer must leave early (Once another Attendee becomes an Organizer this privilege cannot be revoked.)

## Presenter privileges

A Presenter is the user actively sharing his or her desktop screen with other Attendees. Only one Attendee at a time within a session may be granted the active Presenter role. Presenters have the following controls available to them:

- The ability to enable, disable or pause screen sharing, which can be helpful to avoid displaying confidential data that might otherwise appear on the Presenter's desktop (e.g., while searching files or folders)

- The ability to grant/revoke remote keyboard and mouse control to another Attendee, which facilitates efficient communication through desktop interaction
- The ability to make another Attendee the Presenter, providing for a flexible, dynamic flow during sessions

Whenever a Presenter is sharing his or her screen with other Attendees, an "On Air" indicator is displayed on the Presenter's Control Panel. To share his or her screen, the Presenter must click the "Show My Screen" button on the Control Panel. These features ensure that Presenters always know when desktop sharing is active so that desktop screens are never shared accidentally.

### Attendee privileges

Users with the basic Attendee role have the following privileges:

- The ability to join any session to which they have been invited at or after the session's start time
- The ability to view the Presenter's screen unless the Presenter has paused or disabled screen sharing
- If granted, the ability to remotely control the Presenter's keyboard and mouse (Remote control privileges are automatically revoked whenever the active Presenter role is changed.)
- The ability to use Chat to send text messages to all other Attendees or to one specific Attendee (Chat may be disabled for one or more Attendees by an Organizer.)
- The ability to leave a session at any time

Basing access rights and privileges on assigned roles allows flexible sessions that facilitate highly dynamic interaction between Attendees, without sacrificing either control or visibility. Organizers can easily add Attendees or change the Presenter as needed throughout the session. Presenters remain in complete control of their own desktops, and Organizers have everything required to manage the session effectively.

## Account and session authentication features

Role-based authorization depends upon the ability to correctly identify and authenticate every user. To ensure that each Organizer, Presenter and Attendee is in fact who he or she claims to be, GoToMeeting, GoToWebinar and GoToTraining incorporate robust account and session authentication features.

### Web site account login

To access a user account on the GoToMeeting, GoToWebinar and GoToTraining Web site, users must supply a valid email address and corresponding user account password. To make them hard to guess, all passwords must contain at least eight characters and include both letters and numbers. Too many failed log-in attempts cause the Web site account to be temporarily locked to protect against password guessing. Passwords stored in the service database are encrypted and checked using a cryptographically secured verifier that is highly resilient to offline dictionary attacks.

## Session information disclosure

Unlike some competing solutions, information describing scheduled GoToMeeting, GoToWebinar and GoToTraining sessions is only available to the Organizer and invited participants. Because session descriptions are only displayed after users have successfully authenticated, and then only to those users authorized to view it, potentially sensitive information such as the session subject, Organizer name and session time are never exposed for casual perusal by hackers, curious Web surfers or your competition.

## Authentication of session attendees

Because most organizations hold many sessions with restricted attendance, it is not enough to let any user associated with a given GoToMeeting, GoToWebinar or GoToTraining account view session descriptions or attend sessions. Instead, authorization to join each session is based on a unique Session ID and an optional Password.

Whenever a session is scheduled, a unique nine-digit Session ID, created by the GoToMeeting, GoToWebinar or GoToTraining service broker using a pseudorandom number generator, is returned to the Organizer. The Session ID is then communicated to all invited Attendees using email, instant messaging, a telephone or other communication methods.

To join the session, each Attendee must present the Session ID to the service broker by either clicking on a URL that contains the Session ID or by manually entering the value into a form presented by the downloaded GoToMeeting, GoToWebinar or GoToTraining client.

Whenever a valid Session ID is presented, the service broker returns a set of unique session credentials to the GoToMeeting, GoToWebinar or GoToTraining client. These session credentials are never seen by the Attendee, but are used by the software to connect to one or more communication servers. Credentials include a 64-bit Session ID, a short Role ID and an optional 64-bit Role Token. These are used to identify the appropriate session and transparently authenticate the user as either an Organizer or Attendee. All sensitive communications take place over SSL-protected connections to prevent disclosure of session credentials.

In addition, Attendees must authenticate “end-to-end” with the session’s Organizer. This is based on a secret random value provided by the service broker and an optional Password that the Organizer chooses and communicates to Attendees. To provide maximum assurance against unauthorized access and ensure session confidentiality, Citrix Online strongly encourages the use of the Password feature.

It is important to note that the optional Password is never transmitted to Citrix Online at any time. This provides added assurance that no unauthorized parties, including Citrix Online operations personnel, can join and participate in the session.

“End-to-end” authentication is accomplished using the Secure Remote Password (SRP) protocol. SRP is a well-established, robust, secure password-based authentication and key exchange method. SRP is resilient against a wide variety of attacks, including both passive eavesdropping and active password cracking. (More information on SRP may be found at http://srp.stanford.edu.)

By providing two levels of Attendee authentication, GoToMeeting, GoToWebinar and GoToTraining ensure that only authorized Attendees can join sessions to which they have been invited, and that each user is granted privileges inaccordance with his or her assigned role.

## Administration-site security

Like all connections to the GoToMeeting, GoToWebinar and GoToTraining Web site, connections to the administration portal are protected using SSL/TLS. Administrative functions are protected using strong passwords, activity logging, regular audits and a variety of internal physical and network security controls.

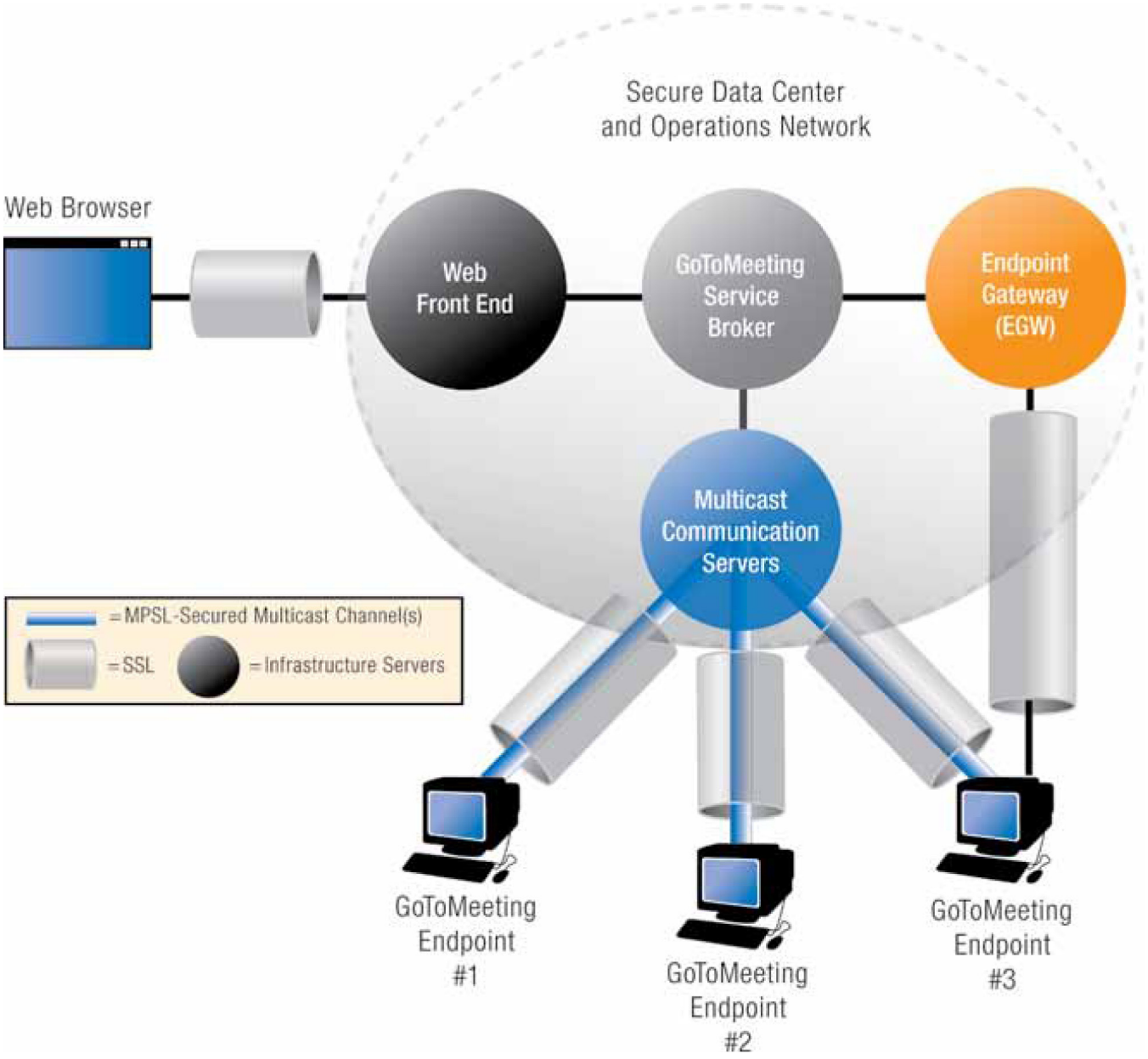


Figure 2

# Communications security features

Communication between participants in a GoToMeeting, GoToWebinar or GoToTraining session occurs via an overlay multicast networking stack that logically sits on top of the conventional TCP/IP stack within each user's PC. This network is realized by a collection of Multicast Communications Servers (MCS) operated by Citrix Online. This communications architecture is summarized in Figure 2.

Participants (session endpoints) communicate with Citrix Online infrastructure communication servers and gateways using outbound TCP/IP connections on ports 8200, 443 and 80. Because GoToMeeting, GoToWebinar and GoToTraining are hosted Web-based services, participants can be located anywhere on the Internet — at a remote office, at home, at a business center or connected to another company's network. Anytime, anywhere access to the GoToMeeting, GoToWebinar and GoToTraining services provides maximum flexibility and connectivity. However, to preserve the confidentiality and integrity of private business communication, these tools also incorporate robust communication security features.

## Communications confidentiality and integrity

GoToMeeting, GoToWebinar and GoToTraining provide true "end-to-end" data security measures that address both passive and active attacks against confidentiality, integrity and availability. All connections are "end-to-end" encrypted and accessible only by authorized session participants.

Screen-sharing data, keyboard/mouse control data and chat information are never exposed in unencrypted form while temporarily resident within Citrix Online communication servers or during transmission across public or private networks.

Communications security controls based on strong cryptography are implemented at two layers: the "TCP layer" and the "Multicast Packet Security Layer" (MPSL).

## TCP layer security

IETF-standard Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are used to protect all communication between endpoints. To provide maximum protection against eavesdropping, modification, or replay attacks, the only SSL cipher suite supported for non-Web-site TCP connections is 1024-bit RSA with 128-bit AES-CBC and HMAC-SHA1. However, for maximum compatibility with nearly any Web browser on any user's desktop, the GoToMeeting, GoToWebinar and GoToTraining Web site supports in-bound connections using most supported SSL cipher suites.

For the customers' own protection, Citrix Online recommends that customers configure their browsers to use strong cryptography by default whenever possible and to always install the latest operating system and browser security patches.

When SSL/TLS connections are established to the Web site and between GoToMeeting, GoToWebinar or GoToTraining components, Citrix Online servers authenticate themselves to clients using VeriSign/Thawte public key certificates. For added protection against infrastructure attacks, mutual certificate-based authentication is used on all server-to-server links (e.g., MCS-to-MCS, MCS-to-Broker). These strong authentication measures prevent would-be attackers from masquerading as infrastructure servers or inserting themselves into the middle of session communications.

## Multicast layer security

Additional features provide complete "end-to-end" security for multicast packet data, independent of those provided by SSL/TLS. Specifically, all multicast session data is protected by "end-to-end" encryption and integrity mechanisms that prevent anyone with access to our communications servers (whether friendly or hostile) from eavesdropping on a session or manipulating data without detection. This added level of communication confidentiality and integrity is unique to our products. Company communications are never visible to any third party, including both users who are not invited to a given session and Citrix Online itself.

MPSL key establishment is accomplished using public-key-based SRP-6 authenticated key agreement, using a 1024-bit modulus to establish a wrapping key. This wrapping key is then used for group symmetric key distribution using the 128-bit AES-CTR algorithm (see http://srp.stanford.edu/design.html). All keying material is generated using a FIPS-compliant pseudorandom number generator seeded with entropy data collected at runtime from multiple sources on the host machine. These robust, dynamic key generation and exchange methods offer strong protection against key guessing and key cracking.

MPSL further protects multicast packet data from eavesdropping using 128-bit AES encryption in Counter Mode. Plain text data is typically compressed before encryption using proprietary, high performance techniques to optimize bandwidth. Data integrity protection is accomplished by including an integrity check value generated with the HMAC-SHA-1 algorithm. Because GoToMeeting, GoToWebinar and GoToTraining use very strong, industry-standard cryptographic measures, customers can have a high degree of confidence that multicast session data is protected against unauthorized disclosure or undetected modification.

Furthermore, there is no additional cost, performance degradation or usability burden associated with these essential communication security features. High performance and standards-based data security is a "built-in" feature of every session.

## Firewall and proxy compatibility

Like other Citrix Online products, GoToMeeting, GoToWebinar and GoToTraining include built-in proxy detection and connection management logic that helps automate software installation, avoid the need for complex network (re)configuration, and maximize user productivity. Firewalls and proxies already present in your network generally do not need any special configuration to enable use of our Web conferencing tools.

When GoToMeeting, GoToWebinar or GoToTraining endpoint software is started, it attempts to contact the service broker via the Endpoint Gateway (EGW) by initiating one or more outbound SSL-protected TCP connections on ports 8200, 443 and/or 80. Whichever connection responds first will be used and the others will be dropped. This connection provides the foundation for participating in all future sessions by enabling communication between hosted servers and the user's desktop.

When the user attempts to join a session, the endpoint software establishes one or more additional connections to Citrix Online communications servers, again using SSL-protected TCP connections on ports 8200, 443 and/or 80.

These connections carry data during an active session.

In addition, for connectivity optimization tasks, the endpoint software initiates one or more short-lived TCP connections on ports 8200, 443 or 80 that are not SSL protected. These network "probes" do not contain any sensitive or exploitable information and present no risk of sensitive information disclosure.

By automatically adjusting the local network conditions using only outbound connections and choosing a port that is already open in most firewalls and proxies, GoToMeeting, GoToWebinar and GoToTraining provide a high degree of compatibility with existing network security measures. Unlike some other products, ours do not require companies to disable existing security measures to allow Web conferencing communication. These features maximize both compatibility and overall network security.

## Endpoint system security features

Web conferencing software must be compatible with a wide variety of desktop environments, yet create a secure endpoint on each user's desktop. GoToMeeting, GoToWebinar and GoToTraining accomplish this using Web-downloadable executables that employ strong cryptographic measures.

### Signed endpoint software

Our client endpoint software is a Win32 executable that is downloaded to users' computers. A digitally signed Java applet is used to mediate the download and verify the integrity of the GoToMeeting, GoToWebinar or GoToTraining endpoint software from Citrix Online servers. This protects the user from inadvertently installing a trojan or other malware posing as our software.

The endpoint software is composed of several Win32 executables and dynamically linked libraries. Strict quality control and configuration management procedures are followed by Citrix Online during development and deployment to ensure software safety. The endpoint software exposes no externally available network interfaces and cannot be used by malware or viruses to exploit or infect remote systems. This protects other desktops participating in a session from being infected by a compromised host used by another Attendee.

### Cryptographic subsystem implementation

All cryptographic functions and security protocols employed by GoToMeeting, GoToWebinar and GoToTraining client endpoint software are implemented using state-of-the-art Certicom Security Builder® Crypto™ and Certicom Security Builder® SSL™ libraries for assurance and high performance.

Use of the cryptographic libraries is restricted to the GoToMeeting, GoToWebinar and GoToTraining endpoint applications; no external APIs are exposed for access by other software running on that desktop. All encryption and integrity algorithms, key size, and other cryptographic policy parameters are statically encoded when the application is compiled. Because there are no end-user-configurable cryptographic settings, it is impossible for users to weaken our security through accidental or intentional misconfiguration. A company that uses GoToMeeting, GoToWebinar and/or GoToTraining can be certain that the same level of Web conferencing security is present on all participating endpoints, regardless of who owns or operates each desktop.

# Hosted infrastructure security features

Citrix Online delivers GoToMeeting, GoToWebinar and GoToTraining using an application service provider (ASP) model designed expressly to ensure robust and secure operation while integrating seamlessly with a company's existing network and security infrastructure.

## Scalable and reliable infrastructure

Citrix Online's service architecture has been designed for maximum performance, reliability and scalability. The GoToMeeting, GoToWebinar and GoToTraining solutions are driven by industry-standard, high-capacity servers and network equipment with the latest security patches in place. Redundant switches and routers are built into the architecture to ensure that there is never one single point of failure. Clustered servers and backup systems help guarantee a seamless flow of application processes — even in the event of a heavy load or system failure. For optimal performance, our brokers load balance the client/server sessions across geographically distributed communication servers.

## Physical security

All Citrix Online Web, application, communication and database servers are housed in secure co-location data centers. Physical access to servers is tightly restricted and continuously monitored. All facilities have redundant power and environmental controls.

## Network security

Citrix Online employs firewall, router and VPN-based access controls to secure our private-service networks and backend servers. Infrastructure security is continuously monitored and vulnerability testing is conducted regularly by internal staff and outside third-party auditors.

## Customer privacy

Because maintaining the trust of our users is a priority for us, Citrix Online is committed to respecting your privacy. A link to a copy of the current privacy policy can be found online at www.gotomeeting.com.

# Conclusion

With GoToMeeting, GoToWebinar and GoToTraining, it's easy to conduct meetings, present information and demonstrate products online to improve business communication. These tools' intuitive and secure interfaces and feature sets make them the most effective solutions for conducting and attending Web conferencing sessions.

Behind the scenes, Citrix Online's hosted service architecture transparently supports multi-point collaboration by providing a secure, reliable environment. As this paper shows, GoToMeeting, GoToWebinar and GoToTraining promote ease of use and flexibility without compromising the integrity, privacy or administrative control of business communication or assets.

# Appendix: security standards compliance

GoToMeeting, GoToWebinar and GoToTraining are compliant with the following industry and U.S. government standards for cryptographic algorithms and security protocols:

- The TLS/SSL Protocol, Version 1.0 IETF RFC 2246
- Advanced Encryption Standard (AES), FIPS 197
- AES Cipher suites for TLS, IETF RFC 3268
- RSA, PKCS #1
- SHA-1, FIPS 180-1
- HMAC-SHA-1, IETF RFC 2104
- MD5, IETF RFC 1321
- Pseudorandom Number Generation, ANSI X9.62 and FIPS 140-2

CITRIX® | online

**Citrix Online Division**
6500 Hollister Avenue
Goleta, CA 93117
U.S.A.
T +1 805 690 6400
info@citrixonline.com

**Media inquiries:**
pr@citrixonline.com
T +1 805 690 2969

**Citrix Online Europe**
**Middle East & Africa**
Citrix Online UK Ltd
Chalfont Park House
Chalfont Park, Gerrards Cross
Bucks SL9 0DZ
United Kingdom
T +44 (0) 800 011 2120
europe@citrixonline.com

**Citrix Online Asia Pacific**
Suite 3201
32nd Floor
One International Finance Center
1 Harbour View Street
Central, Hong Kong SAR
T +852 100 5000
asiapac@citrixonline.com

About Citrix Online
Citrix Online solutions enable people to work from anywhere. Our products include GoToAssist® for remote support, GoToManage™ for IT management, GoToMeeting® for online meetings, GoToMyPC® for remote access, GoToTraining™ for interactive online training and GoToWebinar® for larger Web events.



3.23.10/B-24800/PDF