GD e–Bridge Interpreter Platform – Select Value Points

- ***High definition video*** creates clarity.
- ***One-stop-shop*** for all customer live interpretation and language service's needs.
- ***On demand or scheduled (pre-arranged) cloud based access from anywhere, anytime, to anyone 24/7/365 without costly infrastructure or technology barriers.***
- ***Certified subject matter expert***s in Education, Healthcare and other vertical markets.
- Full and rich media experience that includes ***multi-party video and voice communications, telepresence, multi-screen sharing, text chat, native language recording and editing, web streaming, supported by live language interpretation in over 200 languages.***
- Supports ***concurrent communications across a ubiquitous array of video-enabled devices***, ***operating systems***, ***communications protocols***, and ***user access connections to the Internet***.
- ***Scalable*** from 2 to 100's of users.
- ***Adaptive bandwidth*** enables each participant connection separately and adapts the communication stream for that participant independently from others in the same session, which guarantees the best possible audio and video quality for each user no matter if the participant is on a Smartphone using cellular data or a high-end desktop PC with unlimited bandwidth.
- Enables *each user to meet the way they want, i.e.*, ***to independently configure their view of the conference and to leverage any and all content they want.***
- ***Highest client security protocols in highly-regulated environments*** based on industry standards of HTTPS, SSL and AES encryption providing end to end secure video conferencing with user login and inter-component signaling, media encryption, component authentication (spoof prevention) and session security, and secure firewall traversal (refer to the attachment).
- ***HIPAA compliant*** in support of our hospital and medical clients and their patients' privacy and health information protections.
- ***Low cost per minute*** interpretation services, i.e., customers pay only for the time they actually use with no other fees.
- The only platform of its kind ***capable of serving the vast array of deaf, hard of hearing, and spoken language needs ranging from text to voice to video relay usage***.

Secured Video Conferencing

Connectivity's video conferencing infrastructure is based on industry standards of HTTPS, SSL and AES encryption providing end to end *Secure Video Conferencing*.

At a glance

- AES-128 bit media encryption
- HTTPS with certification login
- TLS with certification for signaling
- New component blocking for spoof prevention
- Encrypted token technology for session security
- No login information kept at the desktop
- Secure Firewall Traversal

User Login and Inter-Component Signaling

With SSL security enabled the portal automatically establishes an encrypted HTTPS channel with each endpoint that attempts to access the system and performs certificate exchange, issued by GoDaddy's as a third party certifying authority. Once certificate verification is completed, login and password information is transmitted securely to the central server over the same encrypted HTTPS channel.

For the client/server application signaling, TLS is employed with key exchange taking place over secured TLS connections and support for the same certificate process as HTTPS.

Media Encryption

To ensure that the content of your conferences cannot be intercepted and decoded without your knowledge, Connectivity's system employs AES-128 bit encryption over SRTP for audio, video, and shared content. A set of keys is used for each form of media for each leg of the conference. The system decrypts and re-encrypts each media stream as it passes through for unprecedented security from one endpoint to the other over public networks.

Component Authentication (Spoof Prevention) & Session Security

Each component in the conferencing system has a unique identifier which is communicated to the system over a secure link and is otherwise not accessible. New components added to the network go to the centralized server for configuration. If no configuration is defined for that machine's specific ID, the machine is blocked from joining the network until the administrator accepts and configures the component.

On the client side, a unique token is generated and encrypted by the central system and sent to the *endpoint* at login over a secured link after the endpoint has sent the central server its unique identifier. The encrypted token is stored by the endpoint and the session is kept alive until the next time the user successfully logs in. Each time the endpoint attempts to access the central server for services (such as call initiation), the endpoint presents its session token to the central server, ensuring that the endpoint is in fact the machine where the credentialed user last logged in.

Secure Firewall Traversal

Connectivity's system provides methods of secure firewall traversal, enabling organizations to leverage the public network to provide GD Interpreter for mobile end users without compromising the integrity of the private network or requiring additional expensive equipment. For implementations where the necessary range of UDP ports are opened on the network, the client uses industry standard ICE/STUN to negotiate UDP ports with our systems servers. These same protocols are employed for NAT traversal.

For implementations where the UDP ports are closed on the network, GD Interpreter uses a proxy solution that overcomes these blocking issues in a secure fashion by tunneling on port 443 using industry standard TCP. The client is able to auto-detect if firewall blocking is taking place and automatically switch to proxy configuration as needed and supports existing hardware-based web proxies.