interprefy

Platform Security

Interprefy offers a robust enterprise communications platform with several layers of built-in security, to provide reliable and secure service to support the most demanding business operations. The platform was built from the ground up with highest level of security in mind.

Application security

The application uses proven industry standards and protocols for encryption. The platform uses TLS 1.2, the safest method available today. It is encrypted and authenticated using AES-128-GCM and uses ECDHE_RSA as the key exchange mechanism.
Regular security reviews and vulnerability tests are carried out by independent security firms, to guarantee highest possible level of security for all platform users. Penetration testing is done in compliance with OWASP 10 methodology.

Transmission security

Interprefy platform is built on WebRTC, the leading technology for secure real-time audio and video streaming from browsers and mobile apps. All media streams sent through Interprefy platform use AES 128-bit encryption, and all stream publishing is taking place from a secure HTTPS page. The main protocols providing WebRTC security are SRTP for media traffic encryption and DTLS-SRTP for key negotiation.
Interpreters and tech support personnel who have access to the event audio and video streams sign NDAs to prevent sensitive information disclosure.

Two-Factor Authentication

Two-Factor Authentication allows the event organiser to limit event access only to users with known phone numbers or email addresses. The list of users should be uploaded when configuring an event. After entering the login token, users need to enter a personal 4-digit code forwarded to them by SMS, phone call or email, depending on the event setting. Event organiser can also allow wider access, limiting access only to users with phone numbers from certain countries/cities, or users with emails belonging to particular web domains (i.e. giving company-wide access).

Event Administration

Event organisers can create unlimited number of events/meetings and have access to a wide range of settings for each event, setting different permission levels for audience and, in some cases, interpreter and speaker tokens. For example, event organisers are able to control access to speaker video, speaker audio, event chat, choose whether user can connect from mobile

apps, etc. Interprefy platform provides an extensive control of admin user permissions as well, allowing to give company admin users access to certain events or to a full company account.

User Management & Control

Customer admins are able to create and delete "read-only" manager users who will have access to login tokens and event settings for events they have been assigned to.
For additional monitoring during events/meetings, moderator interface allows remote support team to control other users. For example, moderators can remotely:

- Control all AV channels and chats
- Control each users' microphone and incoming/outgoing channels
- Control whether audio and video streams are recorded
- Monitor the numbers of users
- Monitor bitrate and packet loss
- Log users out
- Etc.

Network and infrastructure security

Interprefy platform is using a network of multiple redundant servers deployed in different locations. The servers are selected according to the location of participants. Such distributed cloud set-up with extensive global network of servers has an advantage in comparison to local installation, as it allows much higher reliability as well as lower delay and higher quality of audio and video transmission. In case of server failure or attack, service is automatically switching to another running instance or to a replacement instance that was just started.The infrastructure automatically scales its request handling capacity in response to incoming application traffic, further increasing application reliability.
Regular security scans are carried out by independent security monitoring providers.
Most of Interprefy's computing infrastructure is provided by Amazon Web Services, a secure cloud services platform. Amazon's physical infrastructure has been accredited under ISO 27001, SOC 1/SOC 2/SSAE 16/ISAE 3402, PCI Level 1, FISMA Moderate, and Sarbanes-Oxley. Read more about AWS security.

User Data & Logs

All major actions occurring on each event/meeting, such as logins or event setting changes, are logged using user's IP address and username. This information is used for troubleshooting, statistics and fraud prevention.
Interprefy platform is fully GDPR compliant. Personally Identifiable Information is only collected for the admin users. It resides on a secure server that only selected personnel have access to and communication is encrypted using Secure Socket Layer (SSL).