interprefy

INTERPREFY AG

REMOTE SIMULTANEOUS INTERPRETING PLATFORM

SECURITY DOCUMENT

CONFIDENTIAL

DO NOT DUPLICATE OR DISTRIBUTE THIS DOCUMENT WITHOUT WRITTEN CONSENT

Owner	**Joao Garcia**
Version	**V7.0**
Date last reviewed	**08/12/2020**

interprefy

Table of Contents

interprefy

Purpose

The purpose of this document is to demonstrate the security components of Interprefy platform. 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. End-users connect to the platform using variety of interfaces: web browsers, Android and iOS mobile apps, or Windows and MacOS desktop apps.

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-256-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.
Interprefy solution is hosted in Amazon Web Services (AWS) Virtual Private Cloud (VPC). This is a logically isolated section of public cloud where we use resources of a secure virtual network. This is where all meeting data and application resides.

Data transmission security

Interprefy solution is built on WebRTC, the leading technology for secure real-time audio and video streaming for browsers and mobile apps, leveraging a best-in-class telecom provider. All media streams sent through Interprefy solution use AES 256-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.

Event authentication and authorization

Interprefy solution offers several levels of authentication and authorization, for participants joining meetings. These are described below.

interprefy

Single Sign On / Active Directory using SAML 2.0

Interprefy solution offers possibility to integrate with client's single sign on system. In this case, the existing client single sign on system is responsible for verifying the identity of participant requesting approval to join meeting.
It is also possible to restrict the access to meeting to users which belong to a specific Security Group or are whitelisted by meeting organiser.

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 / partners are able to manage users (event managers) who will have access to login tokens and event settings for events they have been assigned to. Managers can only view settings but not modify them.
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.

interprefy

End-user interfaces and permissions

Platform is accessed by end-users through variety of interfaces:

- Interprefy web page
- Android mobile app (available to download from Google Play store)
- iOS mobile app (available to download from App store)
- Windows desktop app (available to download from Microsoft store)
- MacOS desktop app (available to download from Interprefy website)

Only speaker and interpreter roles need permissions to access microphone and camera on the user device. For this, end-user must first provide a valid speaker or interpreter login and then grant mic or camera permission when prompted.
If the app is only used to watch the incoming video or listen to incoming audio, then no microphone or camera permission is needed and request for access is never made.

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 (AWS), 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.

Application user 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 GDPR compliant. It resides on a secure server that only selected personnel have access to and communication is encrypted using Secure Socket Layer (SSL).

Infrastructure audit logs

All changes performed in AWS infrastructure are logged using AWS CloudTrail.

interprefy

Data related topics

Data processed and stored

Interprefy processes and stores the following types of personally identifiable information (PII):
- Meeting setup info: meeting title, name, date/time, email/phone of participants, access tokens
- Meeting attendance info: participants email/phone number, IP address, time participant connected/disconnected
- Meeting audio, video and chats are processed
- Meeting audio and video: when requested by the client or for quality purpose reasons, audio and video from the meeting including audio from interpretation are stored
- Meeting chats

Note: in some cases, event organiser can disable storage of some types data. Production data is not used for development or testing purposes.

Data at rest storage location and encryption

Data at rest is stored in AWS Relational Database Service (RDS) and Simple Cloud Storage Service (S3). Currently Interprefy solution stores data in AWS region Ireland (multiple availability zones).

As per encryption, Amazon RDS encrypted DB instances use the industry standard AES-256 encryption algorithm to encrypt your data on the server that hosts your Amazon RDS DB instances.
For AWS S3, we use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3). When you use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

Data transmission encryption and key

In terms of transmission, all our browser-to-server communication is end-to-end encrypted using HTTPS (HTTP over TLS), and media streams are never transmitted unencrypted on the open internet. Interprefy employs Transport Layer Security (TLS) version 1.2 to encrypt both voice and video data. The core protocols used are SRTP for media traffic encryption and DTLS-SRTP for key negotiation, both of which are defined by the IETF. The endpoints use AES cipher with 256-bit keys to encrypt audio and video, and HMAC-SHA1 to verify data integrity. During the call, media streams are temporarily decrypted while within Interprefy solution cloud servers and then immediately re-encrypted prior to being sent through the internet to the receiving client. This decryption is necessary for transmission optimization and latency reduction.

Data redundancy and backups

Amazon RDS backups are performing every day. Retention period is 7 days.
Amazon S3 provides a highly durable storage infrastructure. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region. Amazon S3 maintains the durability of your objects by quickly detecting and repairing any lost redundancy. If corruption is detected, it is repaired using redundant data.
Backups are performed also in AWS region Ireland in different availability zones.

Data separation

Interprefy solution ensures that each client can only access its data. The separation of data is logical. Data is stored in shared environments.

interprefy

AWS architecture