JULY 2023

HUMMINGBIRDS AI

Technical Specification of Security and Privacy Policy for GuacamoleID Software

V 3.3

This technical specification describes the security and privacy policy of GuacamoleID software. The software is designed to handle facial biometric information in the form of visual telemetry, but no picture or video is recorded or stored. The software encrypts all sensitive data using secure symmetric encryption (AES-256 or stronger) and stores the key in the device's operating system secure credential repository.

The software operates in two modes: Standalone Application and Connected Application

Connected Application, all sensitive information is encrypted during registration and transmission using industry-accepted encryption standards (TLS 1.3 or stronger).

The software does not require internet connectivity except for license validation.

The software also provides options for trusted persons to access the device temporarily.

Personally Identifiable Information (PII) and Sensitive Data

The software collects facial biometric information in the form of visual telemetry, which describes certain non-descript elements of the facial characteristics. The collected information is not sufficient to create a picture or video of the person to identify the person further. No picture or video is recorded or stored. The software does not handle any other Personally Identifiable Information (PII) or sensitive data.

Storage of Sensitive Information

The software collects facial biometric information in the form of visual telemetry, which describes certain non-descript elements of the facial characteristics. The collected information is not sufficient to create a picture or video of the person to identify the person further. No picture or video is recorded or stored. The software does not handle any other Personally Identifiable Information (PII) or sensitive data.

Modes of Operation

The software operates in two modes: Standalone Application and Connected Application.

In Standalone Application, all biometric data stays in the device and is never transmitted over any network.

In Connected Application, a private server is deployed in the local network that connects a group of workstations together.

Registrations (biometric telemetry required for identification) are securely transmitted inside the local network to the server and distributed to other devices in the same local group.

Security Considerations of Connected Application

In Connected Application, all sensitive information is encrypted during registration and transmission using industry-accepted encryption standards (TLS 1.3 or stronger). All nodes authenticate the local group's server by validating a pinned certificate. The server authenticates all registered nodes using a secure ID used for license management and device authentication. Nodes have individual permissions that can be managed on the server to submit new registrations to the server. Nodes can be removed, or their access to adding new registrations can be revoked from the server.

Internet Connectivity

The software requires internet connectivity only for license validation. The software can be deployed in air-tight networks by deploying a local license activation server.

Trusted Access

The software provides options for trusted persons to access the device temporarily. The trusted access options include pausing continuous facial authentication temporarily, allowing access for a certain period of time if the face is recognized, or allowing a third-party face to become trusted by registering that face. The behavior of these options is configurable by the organization's administration.

User Authentication

Within the first few minutes (first 5 minutes by default) after logging in, the software will prompt the user to register their face either if there is no registration or if the face doesn't match. This ensures that the person that authenticated is the same person performing the registration and prevents session hijacking during an active session. If for any reason, the software fails to recognize the user, the easiest way is to log out and log back in so that the face can be registered anew.

Conclusion

In Connected Application, all sensitive information is encrypted during registration and transmission using industry-accepted encryption standards (TLS 1.3 or stronger). All nodes authenticate the local group's server by validating a pinned certificate. The server authenticates all registered nodes using a secure ID used for license management and device authentication. Nodes have individual permissions that can be managed on the server to submit new registrations to the server. Nodes can be removed, or their access to adding new registrations can be revoked from the server.

GUACAMOLE ID

Every Computer Has Chips, It's Time For Guacamole!

For further information and questions, please contact hello@hummingbirds.ai or your sales point of contact.