

BioVox is our speaker verification and identification product. Thanks to its advanced **voice biometrics** technology you can raise the security level in physical or logical access controls and at the same time get rid of magnetic cards and passwords. So you have a double gain: **increased security + user friendly systems**. You can also identify speakers in real time during a phone call.

Because it's **text independent**, **BioVox** is in a different level compared to many other voice biometrics solutions. Users don't need to say fixed pass phrases like "my voice is my passport", so **spoofing attacks are almost completely eradicated** because a different random sequence of numbers can be requested in each login. On the other hand, this ability grants a huge flexibility because **voiceprints can be generated from past free speech recordings**.

BioVox provides an open **SDK (Software Development Kit)** that exports its functionalities through a powerful yet easy to use API (*Application Programming Interface*). With this API you can integrate a complete voice based user validation system into any embedded hardware or software application.

The validation process is done in **two successive steps**, enrollment and validation:

- **Enrollment:** the new user pronounces several utterances, which are then analyzed in order to extract a **voiceprint** that identifies the speaker in a unique way.
- **Validation:** the user to be validated pronounces an utterance (free text, his/her name or a password) which is analyzed and compared with the associated voiceprint, if we're in a speaker **verification** scheme. If they match, the legitimate user is accepted. In the other hand, if the application is working in a speaker **identification** scheme, the utterance is compared with all the voiceprints available and returns the associated user identity, if a match is found.

The open architecture of **BioVox** makes possible a wide range of different applications:

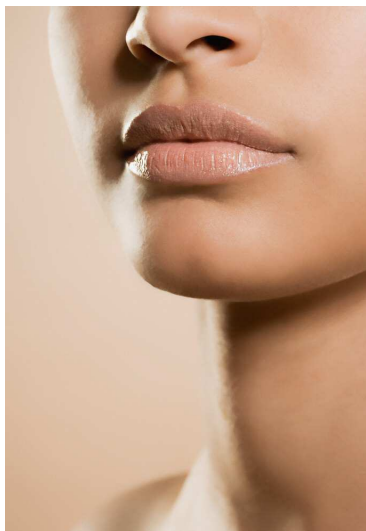
- Security in **call-centers**: continuous identity verification performed in the background.
- **e-commerce & e-banking**: secure payment in Internet, payment with the mobile phone.
- Physical **access controls** and presence controls: no more buddy punching.
- **Alarms and domotics**: electronic devices driven by secure voice commands.
- **Police investigations**, forensic acoustics: identification of suspects in real time.
- **Search for specific speakers in audio recordings**.



PRODUCT

- Text Independent Speaker Verification and Identification System.

KEY FEATURES



- Two matching modes: **verification** (1:1 matching) and **identification** (1:N matching).
- **Text independent.**
- **Language independent.**
- **Security level** can be adjusted.
- Automatic calculation of **quality of voiceprints.**
- Automatic calculation of the **matching score** between the speaker and the voiceprint.
- Two operation modes: **real time** or **batch** mode (file based).
- Highly optimized verification engine: can be integrated into **embedded systems.**

TECHNICAL SPECIFICATIONS

- Audio for enrollment: 30 s minimum, >60 s recommended.
- Audio for validation: 2 s minimum, >5 s recommended.
- Supported audio formats: PCM linear 16 bits 8/16 KHZ, G.711, MP3 (not recommended).
- Voiceprint size: 4 KB.
- Verification (1:1) time¹: < 0.4 seconds.
- Identification (1:N) rate¹: 100 voiceprints analyzed / second.
- EER²: < 1%, dependent of application and system configuration.
- Minimum recommended CPU: Intel i3 3GHz or equivalent.

SUPPORTED PLATFORMS

- Windows® XP, Vista, 7, 8, 10.
- Linux, several distributions.
- Android® NDK.

¹ With minimum recommended CPU.

² *Equal Error Rate*: the value in which the two opposite error rates associated to any biometric system are equal after tuning (whenever one is reduced, the other one is increased as a consequence). These error rates are: *FRR* (False Rejection Rate - a legitimate user is rejected) and *FAR* (False Acceptance Rate - an impostor is wrongly accepted).