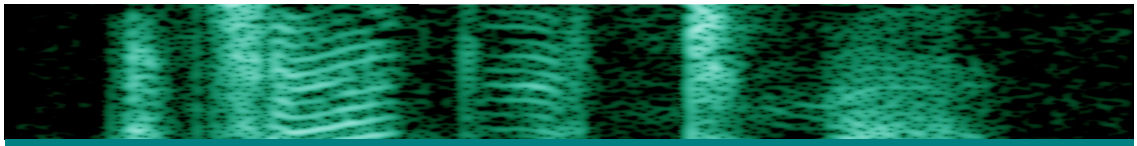


BioVox

Product Information

BioVox is our speaker verification and identification product, **text and language independent**. Thanks to its advanced **voice biometrics** technology you can increase 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 benefit: **increased security** + **user friendly systems**. You can also identify speakers in real time in 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 password*", 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 already available free speech recordings**.

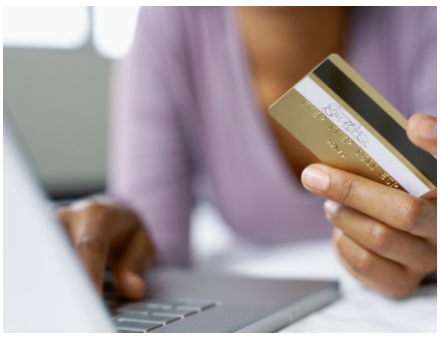
BioVox provides an open **SDK (*Software Development Kit*)** that exports its functionalities through a powerful yet easy to use **API** (*Application Programming Interface*). With this API you can integrate a complete voice based user validation system into any embedded hardware or software application.

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

- **Enrollment**: the new user says a few sentences, which are then analyzed in order to extract a **voiceprint** that identifies that speaker in a unique way.
- **Recognition**: the user to be validated pronounces some sentence (free text, his/her name or a password) which is then 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 on a speaker **identification** scheme, the sentence is compared with all the voiceprints available in the system and returns the associated user identity, together with a N-Best candidate list.

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 or with the mobile phone.

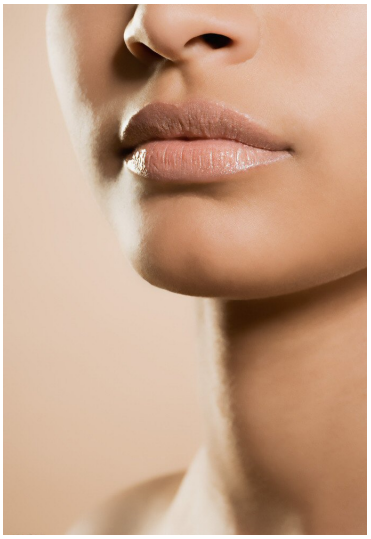


- Physical **access controls** and presence controls: no more buddy punching.
- **Alarms and domotics**: electronic devices driven by secure voice commands.
- **Police investigations**, forensic acoustics: identification of suspects in real time.
- **Search for specific speakers in audio recordings**.

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.
- Feedback about the **quality of voiceprints**.
- Feedback about the **matching score** between the analyzed speaker and the voiceprint.
- **Advanced anti-spoofing technology**: protection against voice recorded or text to speech based attacks.
- 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 (recommended), G.711, MP3.
- Voiceprint size: 4 KB.
- Verification (1:1) time[1]: < 0.4 seconds.
- Identification (1:N) rate[1]: 500 voiceprints analyzed / second.
- EER[2]: < 1%, dependent of application and system configuration.
- Minimum recommended CPU: Intel i5, 2.5 GHz w/4 CPU cores or equivalent.

SUPPORTED PLATFORMS

- Windows® 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 made equal (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).