AURAYA

World leaders in voice biometrics

VOICE BIOMETRICS FAQS

This document provides an overview of frequently asked questions regarding voice biometric implementation with ArmorVox.

ArmorVox is Auraya's proprietary voice biometric engine. It is designed with advanced machine learning algorithms and is speaker adaptive. It delivers superior privacy, security and user experience outcomes for businesses and individuals globally.

In this document, we explore technical concepts and common concerns regarding voice biometrics – such as user security and privacy – and how ArmorVox optimizes performance across these measures.

ARMORVOX™

powered by

aws

What is voice biometrics and how does it work?

Voice biometrics is a speaker authentication technology that captures a voice sample from a live speaker and compares it to a previously stored voiceprint to produce a voice-match score of the voice sample with the voiceprint.

An ArmorVox voiceprint identifies 3,900 unique characteristics per second of speech, which represents the unique acoustic “signatures” in voice associated with the speaker’s vocal tract and other anatomical characters, habitual speaking style (such as accents and language) as well as cadence and pitch. Independent research has shown that a voiceprint is unique to an individual, just as a fingerprint is.

Where are voiceprints stored?

ArmorVox voiceprints are encrypted and stored in a secure database behind the firewall. This database cannot be accessed other than via the voice biometric system which itself is protected behind a firewall.

The voiceprint database is doubly secured from attack. In addition, in ArmorVox personally identifiable information, such as voice files and identity credentials are removed from the system, ensuring compliance with GDPR and other security regulations.

What about privacy concerns? Are consumers aware that their voice is being recorded?

Auraya Systems is a founding member of the Biometrics Institute which sets the industry best practices for organizations using biometric technologies. Customers can choose to use their voice for identity verification and access and they have the option to opt out. They can also delete the voice biometric after enrolment where required which is a function integral to ArmorVox.

Disclosing use of voice biometrics has helped our customers differentiate themselves in their respective markets. While PINs and passwords continue to fail, and hacks and breaches climb, organizations that are deploying voice biometrics show that they are truly innovating the customer experience, and taking their customers’ security seriously.

Can the system be “hacked?” Specifically, what if I recorded your voice, then played it back to a voice biometric system and pretended to be you? Can I fool the system easily this way?

ArmorVox ensures that a system cannot be breached by a recorded playback of a person’s voice. Liveness Detection using random challenge response can quickly flag whether the spoken voice is a recording or a live person, or whether speakers have changed between verification and on-going service delivery.

What about an impersonator? Or identical twins? Can they easily trick the voice biometric system?

ArmorVox analyses 3,900 voice characteristics every second while matching it against a voiceprint – this is unique to each person. This includes both physical characteristics – the size and shape of the larynx or nasal cavity, for example – and behavioral characteristics – rhythm of speech, intonation, accent, etc.

While behaviors can be easily mimicked, physical voice characteristics cannot, and this prevents impersonators or identical twins from “tricking” the system. ArmorVox also employs patented methodologies and machine learning to actively learn a user's voice with frequent use. It ensures highly accurate matching of a person’s voice against their unique voiceprint and tracks near neighbor voiceprints.

What if I have a cold? Won’t the system fail? If the voice biometric system should fail, is there a backup in place?

Normal fluctuations in a person’s voice won’t adversely cause a voice biometrics system to fail. However, if someone has a physical ailment such as laryngitis or a more severe illness which causes an inability to speak, voice biometrics technology will obviously be challenged.

In this case, customers would simply revert to another biometric on their device (if offered), or to a series of authentication questions. This depends on how the system is designed.

What is the benefit to a customer?

The overall objective of implementing voice biometrics is to increase client convenience for authentication and to enhance security. Voice biometrics eliminates the need for PINs, passwords or security questions, and makes it possible for customers to speak a simple voice pass phrase for identity authentication.

How secure is it?

Voice biometrics technology can be used as a multi-factor authentication (something you know, which is the passphrase, and something you are, which is your voice). The security of the ArmorVox system has been shown to be the strongest in the industry.

Armorvox's proprietary speaker adaptive machine learning algorithms constantly check the security of a voice print against other speaker in the system to continuously optimize accuracy and uniqueness of the voice print. Because of this, ArmorVox can identity weak voiceprints making it is less susceptible to fraud threats that affect other voice biometric systems and more traditional methods of authentication such as PINs and passwords.

With the voice biometrics system that is in place, is it possible for somebody else to be falsely accepted on my account?

No biometric system or security system is 100% fool-proof. ArmorVox implements Impostor Maps; a patented approach that measures the possibility of a voiceprint falsely accepting an incorrect speaker for the true speaker upon single or multiple attempts.

This enables the thresholds and business rules to be individually set for each voiceprint enrolled to maximize security for that speaker. This way the security performance of the overall system can be set to meet the business requirements. The voiceprints are continuously tuned and optimized over time as speakers verify and the system captures more characteristics unique to the speaker’s voice.

How can you prevent someone being falsely accepted into my account?

ArmorVox implements multiple layers of security to prevent impostor speakers or “false accepts”.

This includes prompting users for additional voice samples and locking user accounts after multiple failed access attempts. Leveraging multiple layers of security, especially for high-risk transactions, is another best practice.

Shouldn’t voice biometrics be able to identify each and every person as unique? If there is even a remote chance of a “false accept,” isn’t it risky to use voice biometrics?

We’ve seen PINs, passwords and security questions lead to massive-scale data breaches at some of the largest organizations in the world. Time and again, passwords are stolen and massive amounts of data are compromised, putting consumers at risk. ArmorVox is proven to reduce security risk and to drive down fraud, while at the same time offering a more convenient user experience.

Can a voiceprint enrolled in one channel be used in another channel? For instance, can voice prints enrolled in a browser be used to authenticate the same customer to access call center or help desk services?

ArmorVox uses a client-server architecture with published APIs across all customer service channels. Solutions using ArmorVox can enrol speakers in one channel and verify them in the same or different channels.

A customer can enrol through a smartphone application or website. Once enrolled, the voiceprint can authenticate the customer across other channels as well. Similarly, voiceprints can be captured during a telephone call, which can then be made available in digital channels providing customers with the same authentication experience across all customer channels.

Can a voice biometric system support multiple modes and biometric security?

ArmorVox implements all voice biometric modalities, text-dependent, text-promoted and text-independent voice biometric in a single software license. This allows users to combine set-phrases, random channel responses and conversation speech voice biometrics to meet their specific user experience and business requirements. Further, users can start of with a simple set-phrase solution and then expand this to implement different modalities as customer requirements expand without having to re-engineer the solution. In effect, the approach future proofs voice biometrics solutions based on ArmorVox.

Do we have to re-enroll users when we upgrade the voice biometric system?

ArmorVox voice prints are always backwards compatible.

Can we use the voiceprints from our existing legacy voice biometric system in ArmorVox?

ArmorVox implements tools and methodologies to upgrade voiceprints from your existing legacy voice biometric system to ArmorVox.