voicevault

Mobile Voice Biometrics as a Unified Approach

Harnessing the power of voice to eliminate the need for passwords to deliver convenient identity verification solutions to mobile users without compromising security.

voicevault

Connect with VoiceVault

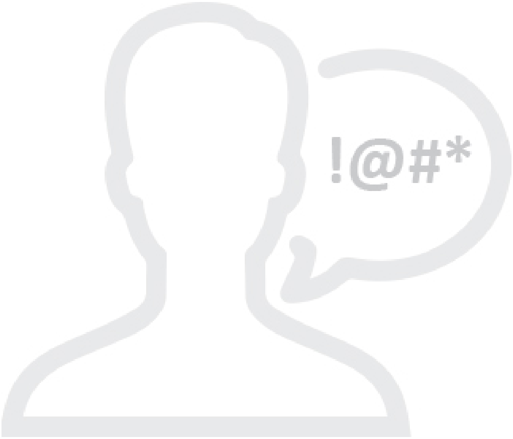
VoiceVault Inc.
400 Continental Blvd.
6th Floor
El Segundo, CA 90245
USA

info@voicevault.com
www.voicevault.com
310.426.2792

voicevault

Table of Contents

Introduction



Mobile users are increasingly frustrated

at having no alternative to the typing in of their passwords that are gaining in complexity in their requirements for hard-to-crack character combinations (upper case… lower case… special characters… minimum length...). Organizations are therefore looking for new ways to eliminate the need for these passwords to deliver convenient identity verification solutions to their users without compromising security.

Voice biometrics is a natural fit for mobile apps simply because speaking into a mobile device is completely natural and intuitive for the end user. They are also a straightforward solution to the 'convenient security' requirement that organizations have for identity verification. It is no surprise then that users like having a choice when logging in or verifying a transaction (or whatever): if it's convenient, they can user their voice; or if it would be awkward to speak, they can type in their password.

Providing a way for organizations to integrate voice biometrics into their apps and for those apps to be readily deployable requires a paradigm shift in thinking and vendor product offerings.

This white paper aims to define what this shift needs to be and why it will make your deployment of mobile voice biometrics much easier in terms of your time, your resources and your money.

The idea is simple: a unified product offering that simplifies the decision-making process and facilitates integration and deployment of voice biometrics in mobile apps.

Why Voice?
Top Three Reasons:

1

We all have devices and we all speak into them without a second thought because it’s a natural and effortless thing to do.

2

High levels of security and convenience can be delivered in a straightforward and device independent way which makes voice popular with developers and those responsible for security.

3

Consumers like voice as there is nothing to remember (the short phrase is right there on the screen) and there’s nothing to type in - a frequently burdensome activity on a mobile given the need for typed passwords to be complex if they are to provide any kind of security.

So, What is It?

The Unified Approach

is one that is designed so that you can benefit from standardized settings and services that are tailored to a single and specific use case, referred to in this white paper as the use of voice biometrics within a mobile app for user identity verification.

The purpose and benefit of such an approach is that all use cases are treated the same – whether voice biometrics are being used to login to an app, or authorize a transaction for example. The security and convenience goals are the same and therefore the apps can use the same underlying settings and underlying system infrastructure.

In practice this means that there is much less work all round (for you and for the vendor) in understanding what the right settings to use in your specific scenario are. You're able to use the off-the-shelf settings knowing that they will meet your needs. The one-size-fits-all approach is based on a large amount of vendor data analysis for how voice biometrics have been applied in real-world production apps to determine the optimum settings to use.

A unified approach takes the view that deployment goals are common: the need for high levels of security that are not at the expense of user convenience. In other words, the settings employed for voice registration and verification can be standardized.

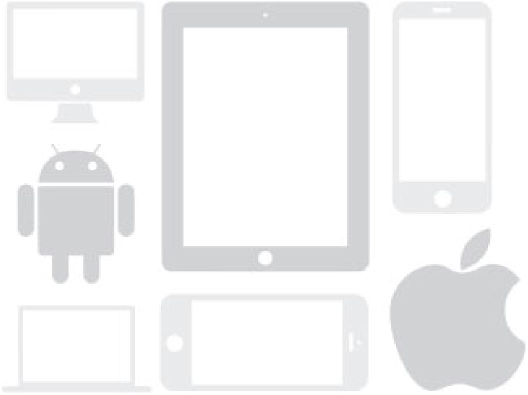
There are generally a range of stakeholders involved in making decisions surrounding technology for core initiatives such as mobile identity verification and they all need to know that their needs and responsibilities are covered. A mobile authentication ecosystem will be stakeholder-aware and accommodate all of their needs (and of course provide readily-available materials to answer questions and get stakeholders on board). If this weren't the case, one of the key benefits of such an approach would be lost – the ability to make a GO decision quickly on integration and technology deployment.

Information on every aspect of the approach

Must be available up front:

- ✓ Pricing and contract
- ✓ Development platform and sandbox
- ✓ Cloud storage (and its security and compliance standards)
- ✓ Documentation (technical, educational and stakeholder)
- ✓ Integration best practices and deployment guidelines
- ✓ Rollout marketing support (end-user education on voice biometrics for example)

Why Mobile Apps Make the Case for a Unified Approach



Use Case Commonality

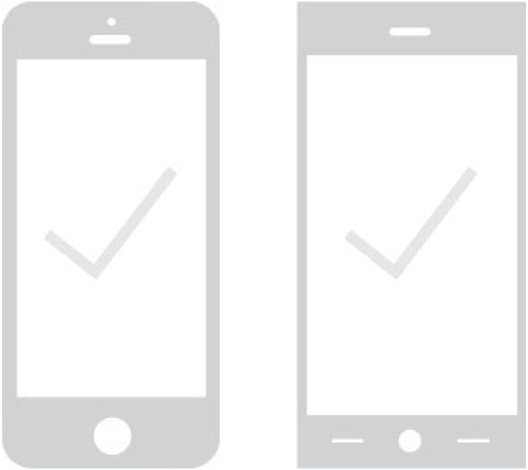
There is a very wide range of smartphones and tablets on the market, and the people using them are a diverse bunch who use their devices anywhere and at any time. There is a huge amount of commonality however, in the nature and purpose of the security element of the apps that they use. This commonality lends itself to an off the shelf solution that delivers the same high levels of security with ***convenience to everyone***.

Whatever the need for the identity verification step within an app, the voice biometric process that the user goes through is essentially the same (in the same sense that the entering of an old-fashioned password is conducted in the same way by all users): The user registers their voice via the app and then subsequently (at some point in the near future) verifies their identity through the same app, on the same device.

It is this same app / same device / common use scenario that is at the heart of why mobile voice biometrics lends itself to standardization.

Cross-Platform Development Framework

The simplicity of the basic user interface requirements for speech capture within an app also lends itself to standardization. A simple cross platform development framework that packages these basic requirements makes the case for speedy integration and deployment. The need to be able to easily deploy a voice biometric app across devices, platforms and operating systems is a key driver for a unified approach to mobile voice biometrics.



What are the Benefits of this Approach (how do you save time and money)?

No Need to Learn the Intricacies of Voice Biometrics

There are several reasons for adopting this sort of implementation methodology and, while they fundamentally come down to a saving of time, money and resources, the elimination of the need to learn about the technical underpinnings of voice biometrics is a major factor in accelerating an implementation.

No Need for Trials or Data Analysis

As with any technology based on statistical methodologies, such as voice biometrics, where 'performance' is largely measured on the accuracy of the solution in the real world, there is a tendency to require the 'proving out' of the claimed metrics in a trial. An organization will usually require to 'see for themselves' that the technology stacks up to the vendor claims. Such trials require statistically significant numbers of participants (typically 1000s of people) and therefore take a considerable amount of time to conduct (not even counting the data analysis at the end of the trial).

One of the benefits of pre-configured settings in a standardized product is that the settings are based on extensive data analysis of the technology being used in the specific use case for which the product is designed – in this case, mobile apps. As such, the vendor has already done the trialing and analysis so repeating it within an organization (with that organizations' users, devices, apps, use case etc.) would yield exactly the same results.

What is Voice Biometrics

Voice biometrics is the simple process whereby a users is able to verify their identity by speaking a short phrase that is then compared to phrases that they provided when registering their voice. This process is possible as all our voice are unique.

Voice registration takes about 20 seconds and verification around 5 and these processes can be conducted from any phone and from anywhere. Mobile apps are of course very well suited to voice biometrics as the app prompts the user for the phrase they need to say on the screen, and users find it very natural to speak into their phone.

Deployment Team Stays Focused on Their Areas of Expertise

A voice biometric development platform helps to keep your development team focused on their areas of expertise – that of building beautiful apps that your customers want to use. A platform that insulates them from the inner workings of the technology and provides the necessary voice capture user interface elements means that they will spend less time building voice biometrics into your app.

Vendor Passes on Cost Savings

There's no denying that a unified offering of a one-size-fits-all product saves the vendor money (for a start, less time is spent helping a client customize a solution to their exact needs), and this will be passed on to the client for the benefit of all. Everyone saves in having such an approach – everyone's costs are lower.

Stakeholder Objections Handled Early

In order for integration and deployment to be a straightforward process, it's important that all project stakeholders have their needs and concerns addressed up-front so that decisions can be effected efficiently. A unified approach therefore needs to have in place, and readily available, all of the materials needed to allay any concerns that each of the stakeholder roles has. Being able to address stakeholder needs up front will save a lot of time in the long run.

Minimized Customization Decisions

A product that offers a range of settings and configurations will require some level of analysis by the client organization or vendor as to which one to select. While this may have advantages under certain circumstances, the analysis process will take time, expertise and resources. A truly great unified product will provide the minimum amount of customization and configuration. The less choice you're given, the quicker it is to pick the settings you're going to use.

No Need for Local Infrastructure

The need to provision local hardware, and tie-up local expertise to install and manage it, is always a big drain on project resources. The use of a plug-and-play cloud-based system within a unified product greatly minimizes the time and money that must be expended to support a solution.

This is especially true if reporting and system management etc. is web-based and self-service with no requirement for back-end system integration.

Of course it's important that the cloud-based system is trusted and supports all of the necessary and relevant industry standards for security and compliance such as PCI DSS.

Getting the Benefit of a Unified Product

To Maximize a Unified Voice Biometric Product

you need to think smart. You'll know that the unified product is a good one if it enables you to do all of the following easily, quickly, efficiently and with the minimum of fuss. When making the decision, you're buying into the off-the-shelf approach so adopt as much of the off-the-shelf product as you possibly can – this is where you will reap the rewards of your decision.

Socialize the demo and use it to decide on how you are going to integrate voice biometrics into your mobile app.

Take advantage of the developer framework and cloud sandbox environment, if there is one, along with whatever sample code is available. If your developers need to ask questions about integration, it's good to get them out in the open as soon as possible.

Decide on where in your app the voice biometrics component will fit; what it will replace / supplement; and what you will have your users do if they fail to voice verify (what's the fallback position going to be?). Keep this as simple as possible and use as many of the vendor tools and best practices as possible. Let them do all the work!

Get the appropriate stakeholder materials to your project team – again, having their concerns aired up front will expedite the project. It will also help to educate the team on what's being planned and implemented.

If the approach is as straightforward as it's claiming to be, the pricing model will be simple and easy to understand. Make sure that it is available to you and that there are no hidden extras.

Satisfy yourself that the cloud environment meets your security and compliance standards; and that the SLAs are right for you.

The vendor will know how to help you market the voice biometric solution to your customers. Find out how and leverage it as much as you can.

Check what optional extras are available – you may need to discuss those early in case there is a lead time (for example if you want a nonstandard phrase for enrollment and verification)

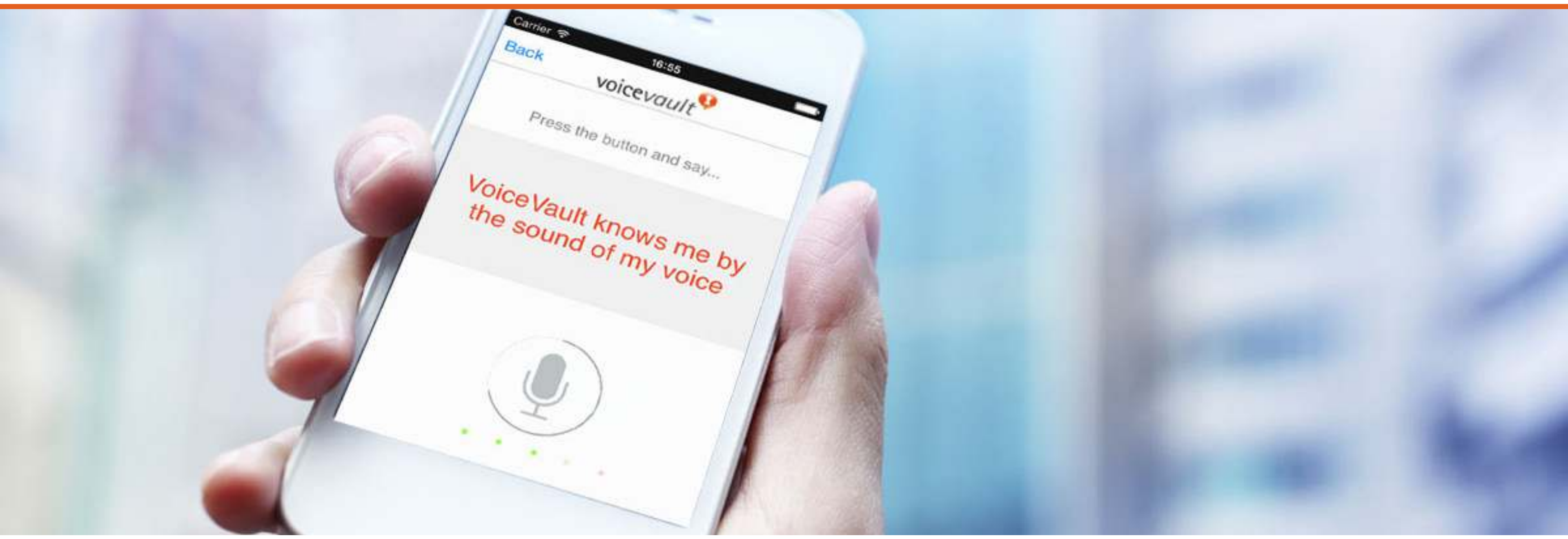
Being based on a SaaS model, the contract will in fact be a service contract. Get a copy early on and make sure it is straightforward and generic (so as to avoid a costly legal review).

What case studies / and reference implementation write-ups are there? Make sure you read them - especially if they relate to your business.

VoiceVault and ViGo

Secured. Simplified. Standardized.

ViGo from VoiceVault is a complete mobile voice biometric product that standardizes each part of the integration, deployment and rollout of a voice biometric-enabled app. It has been designed form the ground up to provide a complete voice biometric ecosystem to enable organizations to deploy mobile solutions quickly and easily saving both time and money.


Carrier
Back
16:55
voicevault
Press the button and say...
VoiceVault knows me by the sound of my voice

The platform provides the cloud-based voice biometric back end; a rapid application development environment; and pre-configured word or digit-based phrases that deliver high security and high convenience. Everything you need to add a voice biometric identity verification step to your mobile Android or iOS app.

ViGo can be incorporated into a multifactor authentication solution for user identity verification for app login, transaction authorization, or any step in a mobile app where authenticating a users' identity is required.

Why VoiceVault?

VoiceVault provides voice biometric solutions for mobile, on-device and telephony applications. The solutions focus on ease of use along with convenience for customers and end-users while providing unparalleled levels of security. Solutions are developed and delivered through partners or direct to client organizations and these can be deployed through a range of hosting models including cloud, on-premise or via managed service providers. VoiceVault's technology is proprietary to them and is 100% in-house developed.

Biometric voice-based solutions enable business processes to enhance multifactor authentication with something you are – *the sound of your voice.*

voicevault