TERMINOLOGY

What is an on-device digital voice and facial print?

A voice and facial print stores the unique characteristics of each person's biometric value.

What is a false negative?

A false negative or false reject is a condition when the voice and facial sample submitted for authentication by the legitimate owner is a weak match against the owner's registered value. Say-Tec on device is configured to deliver no more than a false reject operating point of ~1% when voice and facial recognition are combined. If this condition occurs the person will need to re-authenticate.

What is a false positive?

A false positive or false accept is a condition when the voice and facial sample submitted for authentication by anyone other than the legitimate owner is a strong match against what has been registered. Say-Tec is configured to deliver a 0.0001% false accept rate, which is virtually 100% Authentication success.

PRODUCT

What makes Say-Tec different than other solutions providers?

Say-Tec offers the most complete set of advanced biometric active voice solutions and facial authentication options to meet each company's unique requirements. A simple voice phrase like, "My name is John", along with a facial scan is a very secure consumer step-up authentication. Say-Tec provides unique voice authentication solutions that can identify and authenticate users *simultaneously*. Say-Tec can also extend existing one-time passwords into biometric authentication for superior security and a better user experience. Businesses will not have to worry about record and playback or printed faces because Say-Tec authentication can easily detect these fraudulent schemes.

Can a static phrase be authenticated by Say- Tec?

Yes, The Say-Tec API supports a static phrase value and can also authenticate with facial recognition for on device solutions.

How does the Say-Tec voice and facial authentication work?

Say-Tec utilizes different voice and facial input methods including randomization or a variety of hashing and salting techniques. Say-Tec authentication provides the highest security levels utilizing technology that can't be predicted, replicated, reused, or replayed.

Does a user need to re-register with Say-Tec when using a new phone?

Re-registration is not required, however the company deploying Say-Tec who defines the mobile app functionality may allow a user to port the new phone by accessing their previous voice and facial print.

Does the Say-Tec on device authentication profile expire?

Yes, when the app is removed, or out of date and no longer functioning.

How much does the Say-Tec Authentication service cost?

Say-Tec provides superior convenience, security and service at a competitive price. Please contact the Say-Tec sales team for more details.

How does Say-Tec report a valid or an invalid authentication.

Say-Tec returns an authentication status for each authentication attempt to the app and depending on the result, the user will either be validated or must re-authenticate. The authentication status will need to be considered with other authentication factors for the transaction or activity by the company who offers the app.

What if I want to use a voice passphrase without facial recognition?

Say-Tec recommends using both passphrases and facial recognition for the highest level of authentication security on device.

Please work with your Say-Tec Account representative to discuss Authentication deployment options and pricing.

What are the main advantages of Say-Tec?

Extensibility: Say-Tec enables a user to directly service a function without unnecessary navigation—like paying an invoice or approving a wire by simply authenticating with voice and facial scan

Playback Protection: Say-Tec reduces successful playback potential for fraudulent voice and facial attempts

Security: Robust 3-factor authentication with something each user has (the mobile device), something the user is (unique facial recognition) and something the user knows (voice response).

Is the Voice authentication alpha-numeric?

Say-Tec recommends a numeric and alpha based Voice authentication passphrase.

What is the expected amount of time to register a voice and facial print?

Registration to capture, analyze, store the voice and facial characteristics, and validate should be achievable in 30-40 seconds on device.

What is the expected time to process a voice and facial authentication?

Authentication is instant, with sub second response, and up to a couple of seconds depending on how long it takes to say the passphrase and position the camera for recognition.

How many voice samples are required during registration to determine accuracy during authentication?

The larger the sample size, then generally the greater the accuracy, providing a high-quality registration. Say-Tec recommends Three voice samples, along with the facial scan during registration. Say-Tec automatically and securely stores multiple images of the facial scan.

What is Say-Tec's Operational reliability?

On device authentication is instant, with sub second response, and up to a couple of seconds depending on how long it takes to say the passphrase and position the camera for recognition.

How does Say-Tec know if a fraudster is trying to gain access, with a fake voice, or a printed picture?

Say-Tec uses many tools in evaluating the legitimacy of each user's voice and facial scan. Fraudsters generally will attempt to use replay and synthetic speech generators. However, Say-Tec can identify with the highest accuracy when voice has been modified (speed, pitch, tempo, distortions, noise), spliced audio from multiple utterances, and replayed data using cyclic redundancy checking (CRC). Say-Tec has also been engineered to easily detect printed facial scans, masks, and other fraudulent facial representations.

What is the most important aspect in a high-quality authentication service?

Unlike verifying a binary good/bad password or PIN, voice and facial biometrics are subject to many different and dynamic conditions. For starters, a good registration is essential where the user needs to speak in a quiet location using their natural voice and perform a facial scan in clear lighting. If not, it will result in higher false negatives.

Which mobile platforms are supported by Say-Tec?

Say-Tec supports iOS (7 and later) and Android (Honeycomb or later).

Can a user's voice and facial print be restricted to only one device?

The Say-Tec API controls how devices are associated with each voice and facial print, which is based on the security policy of each company.

Please work with your Say-Tec Account representative to discuss Authentication deployment options and pricing.

Can the Say-Tec authentication be associated with a specific transaction or activity?

Yes, a key advantage of Say-Tec's solution is the ability to uniquely associate it with a specific action. For example, using a bank wire transaction ID, a contract or invoice number or mathematically created token value.

SCIENCE

Is a voice and facial print like a fingerprint?

Voice and facial authentication uses a wide spectrum of audio and video signals that are analyzed, stored digitally, and then compared. Voice and facial biometrics have many more identification reference points than fingerprint and best of all, it works on any phone.

What make up the unique characteristics of each person's voice and facial scan?

The sound of each individual's voice is unique due to the design of their larynx, their physiological make up (tongue, palate, cheeks, nasal cavity, pharynx) and the manner in which the speech sounds are habitually formed and articulated (pitch, tone, language, dialect). The facial characteristics include over 150 measurements and facial angles that uniquely identify the person.

What is the difference between active and passive voice authentication?

The two general types of voice authentication are active, which compares specific spoken voice characteristics like passphrases or spoken digits against a "voice print." Passive voice uses a "voice model" which requires substantially more data to verify a person's voice pattern. Passive voice applies when a voice registration is not available or desirable. Active voice can be verified instantly while passive voice requires considerably more time, and at greater expense. Most importantly, Say-Tec's active authentication service can be used for many more business applications where passive voice is limited to basic call center applications. Please ask your account representative for more information.

What if the user has a cold? Will the solution still work?

The accuracy depends upon the severity of the sickness and the robustness of the voice print. Some voice identifiers do not change with a cold, like cadence and accent that are always measured and compared.

How is the voice and facial authentication result determined?

Voice and facial comparisons are performed against biometric data from the legitimate user that were captured during registration. Authentication of the user are performed with expert engineering to identify the correct match and detect false submissions.

Is the combination of voice and facial authentication better than other biometric authentications such as fingerprint and iris?

Voice and facial authentication works on all devices without special hardware and provides a very high accuracy rate. Please ask your Say-Tec rep for more information and to discuss deployment options.

Does noise impact the ability to process voice authentication?

Voice authentication processing can deal with some acceptable amount of noise. Modern digital phones have noise-cancellation technology which helps improve the voice sample.

SECURITY

Is voice and facial authentication secure?

Yes, a voice and facial authentication is more secure and validates more unique characteristics than a fingerprint. Say-Tec works on any phone using up to 150 unique characteristics of each person's voice and facial scan. Even identical twins can be told apart. Voice and facial authentication can't be stolen like passwords or PINs.

Is my voice and facial print stored securely in the cloud or on device?

Yes, the user's voice and facial print is stored securely on device. When a user submits a request for authentication, The Say-Tec API associates the app, performs the request for authentication and provides an immediate status of the validation.

What if someone else sees the Say-Tec prompt on the user's phone? Can they access their account?

The Say-Tec prompt is only valid for the user who requested it and must be administered by the individual who requested it. Fraudsters will not be granted access.

Is it secure to speak the Say-Tec voice authentication while others are nearby? What if someone overhears?

Speaking Say-Tec authentication prompts are safe because they can not be recorded and replayed to spoof the authentication service. (Static account number-based authentications are not recommended in public settings where someone may hear an account number being spoken.)

What if the user's phone is lost or stolen?

If a lost or stolen phone is used by a perpetrator, they could not use Say-Tec as their voice and facial print will not match.

What if someone records my voice or photographs my face and then plays it back during the Say-Tec authentication prompt?

Say-Tec has various methods to address playback attack and fraudulent facial prints, including unique voice authentication verification, partitioned voice submission and picture detection. A perpetrator would not be able to trick the Say-Tec authentication service.

What would happen if someone else spoke the voice prompt for my approval?

The authentication would be declined based on the voice authentication failure, or in combination with facial recognition.

Is the voice and facial print stored in my phone or in the cloud?

Say-Tec stores the voice and facial print securely on-device, which has the highest accuracy rates, and which is very fast. Please contact a Say-Tec account representative to discuss creating the right solution for your specific needs.

Can someone steal my voice or facial print from my phone?

No, the Say-Tec voice and facial print contains proprietary characteristics of each person's voice and facial scan saved and encrypted as digital bits. If a person's biometric information is ever hacked, it could not be used to recreate that person's biometric identity.

What is the biggest risk with voice and facial authentication?

Ensuring that the registration process is secure and reliable is the single most important part of a biometric authentication program. Companies using voice authentication must thwart fraudsters from gaining access to a voice authentication solution by spoofing an identity and building a fake user profile.

Is Say-Tec single or multifactor authentication?

Being mobile-based. Say-Tec is multifactor. The device itself is a factor and the voice biometrics is a second, and facial recognition is the third factor.

How is the Voice and facial print protected from being associated with each person?

The voice and facial print contains no personally identifiable information. The Say-Tec API holds a unique value that is utilized for authentication.

Can Say-Tec authenticate if the eyes are closed?

No, at least One eye must be open for Say-Tec to authenticate with a facial scan.

Can Say-Tec authenticate if I have a moustache or beard and then shave it off?

Yes, in most cases there will be enough other facial area, including the eyes to properly authenticate. In cases where the beard covers the entire face, a re-registration may be required.

TECHNICAL

What audio formats does Say-Tec support?

Say-Tec supports U-Law, A-Law and Linear PCM.

Is Say-Tec FIDO compliant?

The Fast Identity Online Alliance (FIDO) is a nonprofit consortium formed in 2012 that is working to establish open and scalable standards for authentication systems. Say-Tec works in cooperation with a long list of industry heavyweights to ensure its software solutions align with the organization's expected standards although has not joined the FIDO alliance.

Does Say-Tec use AI or machine-learning?

Yes, each voice and facial print is utilized in an analysis algorithm and over time Say-Tec improves by detecting changes as a person ages, to validate a changing voice and facial scan over time.