Speaker verification planning guide

Introduction

Aculab offers VoiSentry for developers and OEM partners that wish to add voice authentication solutions to any telephony-based application. Aculab's voice biometric engine is a robust, accurate and scalable, API driven solution that easily can be integrated with any business application.

Across all market sectors, businesses compete in terms of customer experience. Enabling the simplicity and convenience of verifying by voice, as an alternative to agent-led ID&V, provides an unobtrusive and intuitive customer experience, in addition to offering heightened security and time/cost savings for the contact centre.

Voice biometrics has gained mainstream awareness in recent times as more and more businesses have been convinced of the advantages that the technology can bring. However, for those business benefits to be realised, a successful implementation is crucial.

The overall success of your implementation project will depend on careful planning, involving several disciplines within your business. Various process owners, including: IT; data protection; HR; sales and marketing; customer services; and the contact centre, need to be engaged from the outset.

This guide is intended to help you to plan the implementation of a speaker verification solution based on Aculab's VoiSentry. By completing the right-hand column in response to the questions posed in the considerations column, you will better able to plan the deployment of your intended solution, because you will have brought into focus the key elements to be addressed during the planning phase.

Consideration	Planning response
Describe the business problem you need to solve, including reference to the impact of maintaining the status quo?	
What metrics will you use to establish the success of the project e.g., customer satisfaction, call handling time, fraud risk, ROI, etc?	
Describe the typical use case(s) where you will use speaker verification?	
Describe any multi-tenant implications where you intend to provide speaker verification as a service to multiple clients or business units?	
How many people will need to have a voiceprint created?	

How many times will each person need to verify against their voiceprint over the course of a year?	
How many verifications per day do you anticipate the system will have to perform?	
What is the maximum busy hour load on your system in terms of inbound calls?	
In terms of calculating the number of verifications per day and the busy hour load, it can help to consider the following: • No. of enrolments? • No. of agents? • Inbound calls per year? • Inbound calls per day? • No. of inbound trunks? • Busy hour traffic (in Erlangs)?	
How will you obtain consent from each person for whom a voiceprint is to be created (note that consent is mandatory per the GDPR)?	
What additional, specific activities do you need to perform to ensure compliance with the GDPR in relation to controlling and processing personal data, including biometric data i.e., voiceprints?	
How will you confirm the identity of each person at the time of enrolment?	
How you will get voice samples from each person for whom you are creating a voiceprint during the process of enrolment?	
Will the method of audio capture be the same for enrolling as for verifying?	
How do you propose to integrate VoiSentry with your existing system(s) e.g., IVR or contact centre front-end (see the *Aculab professional services* flyer and the *VoiSentry API guide* for additional information)?	

What professional services assistance do you need from Aculab (see the *Aculab professional services* flyer for guidance)?	
What advice will you provide to users to ensure you get the best from your deployment (see Aculab's *Tips for training your users* for guidance)?	
Do you intend to store recordings of voice samples provided by each person for whom a voiceprint is created (see the *VoiSentry API guide* for advice on this question)?	
What channels do you anticipate callers using to access the system e.g., landline, mobile (cellphone), VoIP client, etc?	
What languages can your employees/ users/ customers/ subscribers/ clients be expected to use?	
What authentication methodology do you expect to employ (see Aculab's *Best practice guide* for more information)?	
Will you employ multi-factor authentication (see Aculab's *Best practice guide* for more information)?	
What are your intentions regarding the use of passphrases for enrolment and verification (see Aculab's *Choosing your passphrase* for more information)?	
What are your intentions regarding the setting of thresholds for verification of callers (see Aculab's *Best practice guide* for more information), bearing in mind that implementation will always be a balance between security and convenience?	

What process do you envisage being enacted in situations where a caller fails to be authenticated, through either: i) the valid rejection of an imposter; or ii) the false rejection of a valid user e.g., transferring the caller to a customer representative for additional security questioning (see Aculab's *Best practice guide* for more information)?	
Do you intend or need to run a proof of concept (POC) or pilot implementation rehearsal in advance of full deployment (note that a successful POC can pave the way to a smooth implementation)?	
Describe your plans for internal communication of information, particularly regarding the technology, implications for individual departments, and the deployment process?	