

solutions de service client

Livre Blanc



Guide des meilleures pratiques ::
Réussir le déploiement de solutions
de biométrie vocale

Sommaire

1.	Introduction	3
2.	Etude de cas	3
3.	Conception de la stratégie de vérification.	3
3.1.	Choix de l'empreinte vocale.	4
3.2.	Utilisation ou non d'un texte pour l'empreinte vocale	4
3.3.	Vérification d'arrière-plan ou vérification explicite	4
3.4.	Authentification multifacteur	5
3.5.	Adaptation de l'empreinte vocale	5
3.6.	Test de présence.	6
3.7.	Stratégies de recours	6
3.8.	Comptes à utilisateurs multiples	7
4.	Test du système	7
5.	Lancement du nouveau service	7
5.1.	Promotion	7
5.2.	Inscription	8
5.3.	Après-lancement.	8
6.	Synthèse	9

1. Introduction

Avec plus de 300 clients utilisateurs de sa technologie de biométrie vocale, Nuance est idéalement placée pour conseiller les entreprises souhaitant déployer une solution de vérification vocale. Ce document traite des principaux sujets liés à la biométrie vocale et recommande les meilleures pratiques identifiées.

2. Etude de cas

Une des tâches les plus importantes lors de la conception d'un système de vérification vocale est d'appréhender l'ensemble des considérations commerciales et stratégiques ainsi que de quantifier les avantages potentiels du système.

Généralement, les avantages se répartissent dans les trois catégories suivantes :

- Réduction des coûts d'exploitation grâce à l'automatisation du processus d'identification des appelants ;
- Renforcement de la sécurité permettant de réduire l'exposition à la fraude ;
- Plus grande satisfaction des clients du fait de la simplicité d'utilisation et de l'élimination des contraintes liées aux codes PIN et mots de passe à retenir.

La réalisation d'un audit de sécurité impliquant toutes les parties prises afin d'identifier les objectifs du projet permet aux entreprises de définir la conception optimale de leur système de vérification, y compris le choix des mots de passe, des niveaux de sécurité et des stratégies de dialogue appropriées. Les parties prises incluent les spécialistes de la sécurité, des risques, de la fraude, du service client et de l'informatique. Il convient également de faire le point sur les objectifs et les besoins des appelants amenés à utiliser le système régulièrement.

L'argumentaire pour la justification du service se basera aussi sur les statistiques de performance de déploiements existants utilisant des méthodes de sécurité. Notez que les données d'expériences réalisées en laboratoire reflètent rarement la performance sur le terrain, car elles omettent souvent des facteurs comme les erreurs de correspondance de canaux, le vieillissement de la voix ou encore le comportement de l'appelant.

3. Conception de la stratégie de vérification

Les stratégies de vérification varient en fonction des objectifs de sécurité de l'entreprise. Il convient de trouver le juste équilibre entre sécurité et confort selon le type d'interlocuteur et la nature de la transaction :

- Trouver un identifiant simple à mémoriser et unique pour chaque client - Beaucoup d'entreprises ayant déployé des systèmes de vérification ont privilégié un numéro de compte ou un numéro de téléphone. Compte tenu de la généralisation de la téléphonie mobile, vous pouvez utiliser l'identifiant de ligne d'appel (CLI pour Calling Line ID) comme facteur supplémentaire de vérification de l'identité de l'appelant.
- Utiliser une empreinte vocale à la valeur biométrique forte - Les phrases clés ou les séquences numériques sont les choix les plus courants. Nous y reviendrons plus loin.

Lors de la conception de la stratégie de vérification, tenez compte de la durée de l'enrôlement de l'empreinte. S'il est avantageux pour la sécurité d'avoir plusieurs empreintes vocales et phrases clés pour chaque client, le

processus d'inscription ne doit pas être trop long pour autant, sans quoi vous prenez le risque d'un taux d'abandon élevé et d'une adhésion insuffisante des utilisateurs.

3.1 Choix de l'empreinte vocale

Les séquences numériques présentent l'avantage de réunir la reconnaissance et la vérification en une seule étape, ce que l'appelant appréciera particulièrement. Ainsi, le numéro de téléphone ou le numéro de compte peuvent servir à la fois de justificatif d'identité et d'élément d'empreinte vocale. C'est un parfait exemple de « meilleure pratique » puisque la sécurité est renforcée et le confort d'utilisation optimal.

Autre scénario courant : la rotation des phrases clés. Le système demande à l'appelant de citer une phrase clé différente à chaque appel parmi les 3 à 5 empreintes vocales qu'il aura préenregistrées. Seule limite à cette approche : le nombre de phrases clés nécessaire pour que cette technique soit efficace rallonge la durée de l'inscription. Chaque phrase clé doit être répétée trois fois, ce qui prolonge la durée de l'inscription, introduit une plus grande probabilité d'erreur et présente le risque que l'appelant se lasse et abandonne avant que le processus d'enrôlement soit terminé.

3.2 Utilisation ou non d'un texte pour l'empreinte vocale

Il existe deux grands types d'empreinte vocale :

- Celle dépendante d'un texte : l'empreinte vocale de l'appelant est associée à l'énoncé d'une phrase clé spécifique.
- Celle indépendante du texte : l'empreinte vocale de l'appelant est prise au cours d'une conversation normale, sans évaluation de ce qui est dit.

En d'autres termes, pour la vérification indépendante du texte la comparaison peut porter sur des phrases d'inscription et de vérification différentes.

La recherche montre que la vérification dépendante du texte, avec une phrase clé fixe, est plus rapide et donne de meilleurs résultats que celle indépendante du texte. En pratique, la grande majorité des solutions de vérification de l'identité des locuteurs privilégient les modèles dépendants du texte.

La vérification dépendante du texte est également plus simple pour l'appelant, puisque la phrase clé doit durer 5 à 10 secondes au minimum. Pour la vérification indépendante du texte, l'enregistrement audio de l'appelant est plus long, jusqu'à plusieurs minutes dans le cadre d'une conversation normale.

3.3 Vérification d'arrière-plan ou vérification explicite

La plupart des déploiements commerciaux de solutions de vérification vocale utilisent des méthodes explicites. Le client doit s'inscrire dans le système de vérification et il devra fournir une empreinte vocale pour être authentifié. Cela peut se faire dans le cadre d'un échange oral avec un agent, mais le plus souvent c'est un système automatique de répondeur vocal interactif (IVR pour Interactive Voice Response) qui est utilisé.

La vérification d'arrière-plan suscite de plus en plus d'intérêt. L'inscription se fait lors d'une conversation normale, indépendamment du texte. Les empreintes vocales d'inscription peuvent être extraites de fichiers audio enregistrés.

Parce qu'elle apparaît moins intrusive pour l'appelant, à qui il n'est pas demandé de faire ou de dire quoi que ce soit qui ne lui soit pas familier, la vérification d'arrière-plan peut être vue comme plus pratique. Toutefois,

en raison des limites de la vérification indépendante du texte et du manque d'élément de sécurité dissuasif visible, la vérification d'arrière-plan séduit moins les entreprises soucieuses de renforcer la sécurité et d'améliorer le confort de ceux qui les appellent. Certains problèmes de conformité et de confidentialité liés aux inscriptions en arrière-plan viennent compliquer encore ce type de vérification.

3.4 Authentification multi-facteur

Il arrive qu'un système de vérification vocale ne soit pas totalement sûr de l'identité d'un appelant du fait de la correspondance moyenne de l'empreinte vocale. Cela peut être dû à la mauvaise qualité de l'inscription, un bruit de fond excessif ou des problèmes de signal. Dans ce cas, il est bon de pouvoir récupérer davantage d'enregistrement audio de l'appelant, lui demander de répéter sa phrase clé par exemple (pour la vérification dépendante du texte). Ainsi, la seconde tentative de vérification confirme l'acceptation ou le rejet avec un degré de confiance plus élevé.

Toutefois, dans certains cas, cela ne suffit pas. Le plus sûr est alors de transférer l'appel à un agent pour une vérification plus poussée. Mais le risque est grand que le client soit mécontent ce qui entraînera en plus une augmentation des appels au centre d'appels. Conscient du problème, Nuance recommande d'avoir recours à la vérification des connaissances chaque fois que les correspondances d'empreinte vocale sont incertaines. Il s'agit de poser à l'appelant des questions dont lui seul connaît la réponse pour effectuer la reconnaissance vocale.

Il est prouvé qu'une date secrète, enregistrée au moment de l'inscription, apporte de bons résultats de vérification de connaissances. En effet, c'est un élément d'information :

- Facile à mémoriser,
- Difficile à deviner,
- Présentant un taux de réussite élevé de reconnaissance vocale.

L'association des vérifications d'empreinte vocale et des connaissances permet de limiter considérablement les erreurs dans les applications de vérification. L'authentification multifacteur permet également d'actualiser l'empreinte vocale de l'appelant avec l'enregistrement audio le plus récent, garantissant de meilleurs résultats lors des prochains appels (voir ci-dessous).

Si l'authentification multifacteur peut porter sur toutes les données reconnaissables par un moteur de reconnaissance automatique de la parole, la pratique confirme que l'utilisation d'une date secrète est la plus efficace pour les raisons précitées. D'autres formes de données sont envisageables, mais elles génèrent souvent plus d'erreurs qu'une date secrète. Sinon, il est toujours possible de basculer l'appel vers un agent du système d'identification et de vérification (ID&V), qui demandera à l'appelant des informations qui lui sembleront familières, comme le montant de sa dernière transaction.

3.5 Adaptation de l'empreinte vocale

Le vieillissement du profil vocal peut dégrader progressivement la précision de vérification au fil des ans. Ceci s'explique par les évolutions physiques, la croissance ou le vieillissement, en plus des facteurs psychologiques à long terme. Nuance recommande donc aux clients d'utiliser l'adaptation d'empreinte vocale de Nuance Verifier. Cette fonction procède automatiquement à la mise à jour des empreintes vocales en reprenant les derniers enregistrements audio ayant permis d'obtenir une vérification avec un indicateur de confiance élevé.

Une autre procédure d'adaptation, supervisée cette fois, permet d'actualiser les empreintes vocales après une mauvaise correspondance initiale, ce qui se produit le plus souvent lorsque l'utilisateur appelle avec un autre

téléphone. Si le score de vérification descend en-dessous d'un certain seuil, alors l'appelant devra se soumettre à la vérification des connaissances, indiquer sa date secrète par exemple. Ce second facteur fournit une couche de sécurité supplémentaire et permet d'actualiser l'empreinte vocale à partir des derniers énoncés de l'appelant, ce qui contribue à améliorer les conditions de vérification des prochains appels.

3.6 Test de présence

Comme avec n'importe quel système de vérification vocale, le risque existe qu'un fraudeur utilise des enregistrements numériques d'excellente qualité pour utiliser frauduleusement les voix d'autres personnes et tromper des systèmes de vérification vocale. Même si cela est rare et que les chances de réussite sont faibles, Nuance développe des méthodologies, appelées « tests de présence », pour contrer ce type d'attaques.

Ces tests de présence consistent à demander à l'appelant d'enregistrer une ou plusieurs associations de mots aléatoires au cours de l'inscription. Il doit s'agir d'associations que l'on ne risque pas de trouver dans une conversation normale (comme « vélo banane ») et qui ont de ce fait peu de chances d'être enregistrées. Au moment de la vérification, l'appelant peut être invité à répéter une association de mots choisie au hasard afin de prouver qu'il est réellement présent. Les phrases clés utilisées à tour de rôle fournissent un niveau de sécurité équivalent.

Ces deux méthodes ont néanmoins l'inconvénient de prolonger l'inscription, sans offrir une protection à 100 % contre la fraude, car elles n'augmentent que légèrement le vocabulaire possible. Avec sa méthode de test de présence en vocabulaire étendu, Nuance élimine ces contraintes puisque l'empreinte vocale porte uniquement sur des chiffres. Le test de présence consiste à demander à l'appelant de répéter une phrase unique qui n'est pas constituée de chiffres, celle-ci est comparée en biométrie à l'empreinte vocale existante et le contenu de la phrase est également vérifié par la reconnaissance vocale.

Un des avantages de la vérification indépendante du texte est que le processus d'inscription collecte une grande quantité de données sur la façon de parler de l'appelant. En cours de vérification, l'appelant peut être invité à répéter une phrase sans qu'il ait eu à l'enregistrer lors de l'inscription. La reconnaissance vocale peut porter sur cette phrase pour vérifier que l'appelant a prononcé le bon contenu en plus de l'analyse de son empreinte vocale.

La vérification d'arrière-plan indépendante du texte, par exemple la surveillance d'une conversation entre un appelant et un agent, ne présente pas les mêmes risques d'utilisation d'enregistrements puisque l'agent sert de test de présence et saura rapidement s'il parle à une personne réelle ou non.

Pour résumer, les approches du test de présence sont multiples et plus ou moins efficaces en fonction du contexte. Aux entreprises d'évaluer le risque réel d'attaques à l'aide d'enregistrements pour prendre les mesures appropriées à leur cas spécifique.

3.7 Stratégies de recours

Il est important de concevoir une stratégie de recours appropriée pour les appels que le système de vérification vocale ne suffit pas à authentifier. Cela implique notamment :

- Le transfert des appelants qui n'ont pas réussi à s'inscrire correctement vers des agents en mesure de les guider pour enregistrer une empreinte vocale utilisable.
- Le transfert des appelants soupçonnés d'être des fraudeurs vers une équipe spéciale de lutte contre la fraude.
- L'utilisation de la vérification des connaissances.

3.8 Comptes à utilisateurs multiples

Les entreprises doivent également prévoir une méthode de gestion de l'accès de plusieurs utilisateurs dépendant du même compte. Par exemple, deux membres de la même famille peuvent avoir un compte joint, ou disposer d'un accès équivalent aux services. Il faut donc pouvoir authentifier chacun en utilisant le même numéro de compte.

Dans ce cas, l'identification du locuteur permet de déterminer qui appelle en fonction de la voix, puis d'authentifier la personne d'après l'empreinte vocale enregistrée lors de l'inscription. On part ici du principe que tous les utilisateurs du compte sont inscrits, ce qui n'est pas forcément le cas.

L'identification du locuteur est plus efficace avec de petits groupes (idéalement, moins de dix personnes). Avec un nombre supérieur d'interlocuteurs potentiels, la précision du système diminue.

4.0 Test du système

Il est important de tester la simplicité d'utilisation pour s'assurer que les appelants seront à l'aise avec le système. Avant le déploiement, des experts étudient la simplicité d'utilisation avec des appelants volontaires afin de se faire une idée des conditions des appels, de la voix/personnalité et du rythme de l'application. Généralement, les volontaires correspondent au profil des véritables appelants et ils utilisent une version fonctionnelle de l'application dans un environnement de test où leur comportement peut être observé. L'étude de la simplicité d'utilisation permet ainsi d'identifier les problèmes potentiels et de recommander des solutions pour rendre les conditions d'utilisation optimales avant le véritable lancement.

A la suite du test de simplicité d'utilisation, une phase pilote avec des utilisateurs réels permet d'atteindre le niveau de performance voulu et de définir les seuils de sécurité adaptés. Voici les processus de test généralement utilisés en phase pilote :

- La comparaison de données issues de plusieurs terminaux mobiles ou canaux, dans des conditions sonores variées, avec différents modèles de vieillissement et dans des conditions d'utilisation réalistes.
- Un nombre de situations de test suffisant pour être révélateurs.
- Des utilisateurs qui agissent comme dans des circonstances réelles, et non la simple collecte de données par des participants qui opèrent à partir d'un document écrit.
- Plusieurs tests pilotes pourront être nécessaires jusqu'à parvenir à la stratégie de vérification optimale.

5. Lancement du nouveau service

5.1 Promotion

Il convient de s'assurer que les agents des centres d'appels sont familiarisés avec le nouveau système pour qu'ils puissent en faire la promotion auprès des appelants. Une campagne de lancement interne du nouveau système permet de stimuler l'adoption par les agents et d'en faire des partisans. L'un des principaux avantages aux yeux de l'agent est qu'il passera moins de temps à tenter d'identifier l'interlocuteur et davantage à renseigner les clients, leur proposer d'autres services, etc.

Planifiez une campagne de marketing externe, afin d'expliquer clairement les avantages du nouveau système, en insistant sur la sécurité renforcée et la plus grande simplicité d'utilisation. Des clips audio ou des démonstrations encourageront l'adoption par les utilisateurs.

Assurez aux clients qu'ils auront toujours le choix d'utiliser ou non le système. Constituez des groupes formés à traiter les demandes des clients qui refusent le système.

5.2 Inscription

Prévoyez un moyen d'identifier formellement un appelant avant son inscription, généralement via le serveur vocal interactif ou par le biais d'un agent. Pour plus de sécurité, envisagez également d'envoyer à vos clients un code d'inscription provisoire. Assurez-vous que le script du processus d'inscription est adapté aux attentes de l'appelant et constituez un groupe d'agents qui se chargeront des appels abandonnés.

L'inscription étant généralement intensive pour les serveurs de vérification sous-jacents, songez à étaler l'inscription dans le temps pour éviter de devoir investir dans un grand nombre de serveurs.

L'inscription automatique au moyen d'enregistrements vocaux est également possible. C'est un moyen plus simple et plus rapide d'inscrire de grands nombres de clients. Toutefois, les contraintes de confidentialité et de performance limitent l'efficacité de cette approche dans les conditions réelles.

5.3 Après-lancement

Menez des études de satisfaction après le lancement du système pour interroger vos clients sur leurs impressions et recueillir leurs suggestions.

Les entreprises ont intérêt à ajuster régulièrement leur système pour garantir son bon fonctionnement. Ceci inclut une analyse de la performance du système au regard de l'évolution du comportement des appelants et des évolutions commerciales, ainsi que l'identification des modifications qui permettraient d'améliorer la performance du système, de renforcer la sécurité et de mieux satisfaire les appelants.

La sécurité doit être évaluée régulièrement pour s'assurer que le système est correctement équipé pour résister aux nouvelles techniques d'attaque des fraudeurs.

6. Synthèse

Il n'existe pas de solution unique en réponse à tous les besoins de sécurité des entreprises et à toutes les attentes des appelants. Il convient donc d'accorder l'attention qu'ils méritent à l'ensemble des facteurs couverts par ce livre blanc afin de concevoir un système de vérification vocale suffisamment sécurisé pour lutter contre la fraude tout en restant suffisamment simple pour pouvoir être utilisé par la majorité des appelants.

Les équipes des services professionnels et de conseil aux entreprises de Nuance jouissent d'une grande expérience de ces questions et ont aidé de nombreux clients à les résoudre. Ils sont à votre disposition pour vous aider à concevoir et à implémenter la meilleure solution pour votre entreprise.

Contactez le responsable de votre compte Nuance pour de plus amples détails ou rendez-vous sur www.nuance.com/care