thalesgroup.com

THALES
Building a future we can all trust

Voice Biometrics

to fight fraud and to simplify remote authentication

The multiple challenges of remote authentication

User Experience

The end user experience is an essential element of on-line service delivery. However, it is often compromised by the need to remember or change multiple passwords.

Fight Against Fraud

Remote services are an attractive target for fraud such as identity theft. Global solutions for access must therefore offer robust protection.

Multi Channel

Multiple channels, such as web applications, mobile applications and call centres, are typically employed to enable remote access. They must all combine a best-in-class user experience with rigorous standards of security.

Voice biometrics - the perfect answer

Voice biometrics is the science of using the biological patterns of an individual's voice as a unique means of identification or authentication. Deploying voice biometrics **improves the end user experience** and **strengthens security** by replacing laborious user/password processes with a non-intrusive, seamless identification and authentication experience. Thanks to its natural conversational interface, voice biometrics fits perfectly with multi-channel usage.

The voice is unique to each individual

More than one hundred different voice characteristics can be measured. Some behavioural characteristics, such as rhythm of speech, accent and intonation, can be mimicked. However, voice technology uses physical characteristics that cannot be duplicated, such as the size and shape of the larynx or nasal cavity. It is therefore ideally suited to identifying or authenticating individuals.

Types of voice biometrics

There are two main methods of managing voice biometrics authentication.

Text Dependent Voice Verification

The usual method is for a person to say a specific passphrase, typically about two seconds long and comprising four or five words. User enrollment is then active as the end user must knowingly perform the enrollment and speak the passphrase. The most common scenario is for authentication to be performed via mobile or web.

Text Independent Voice Verification

Thales' solution can support a less intrusive option that does not require the use of a particular passphrase. Instead, approximately thirty seconds of normal, conversational speech is assessed. The typical scenario is to employ this approach to fight fraud at call centres, or for real time passive authentication.

Thales' solution also features **liveness detection.** This identifies 'spoofing' types of attack, such as speech created by fraudsters from recordings of legitimate customers.

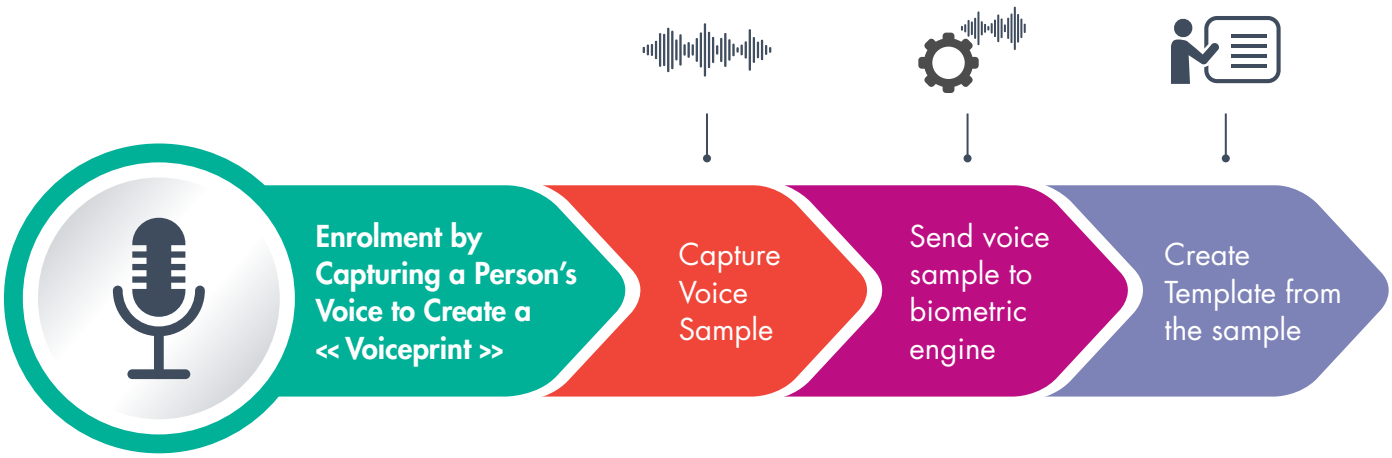
Meeting local regulations

Thales' solution meets local privacy regulations. Individual voiceprints held on the blacklist and weekly call databases are anonymous; they are not linked to named individuals. The solution works by indicating if a caller's voiceprint matches known voiceprints on these databases, thereby demonstrating a risk of fraudulent activity.

Authenticating a legitimate user with voice biometrics

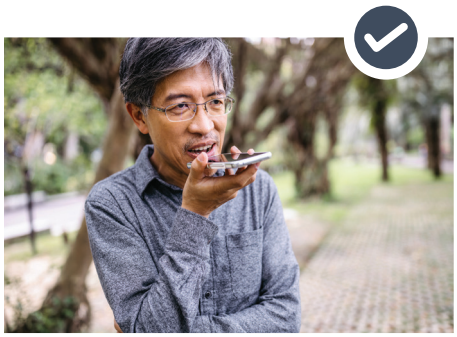
Thales employs a two-step approach: **enrolment** followed by **authentication.**

Step 1: Enrolment: this step aims to verify the identity of a person and bind it to their VoicePrint. A complete voice process is applied, transforming the voice record captured into a digitalized VoicePrint.



Step 2: Authentication: After entering their phone number, the end user is asked to say a passphrase to authenticate. Liveness detection is performed transparently, ensuring the caller is real and not based on a voice record. Final voice authentication is then performed by Thales servers to manage (1:1) voice comparison. If successful the customer is granted access to on-line services.

Using Voice as a Login for Convenience and Security



Detecting fraudulent users at a call centre

The need: The key driver here is **fraud in sales over IVR** (fixed and mobile services). In the call centre channel, there is a pressing need to identify attempts to impersonate genuine end users.

The challenge: Call centres are being contacted by individuals **using different identities** in an attempt to fraudulently access MNO (Mobile Network Operator) services. Current tools for addressing the issue are not effective: they offer call centres **no possibility of detecting impersonation fraud.**

The solution: Operating in SaaS mode, Thales' solution **compares the caller's voice with a blacklist of fraudsters** (in batches, on a daily basis, or through a report).

Automatic splitting of voices from the mono audio channel

Thales' technology works with both mono and stereo recording data.

Our solution can address mono audio, where there is only one channel in the audio for both the voice of the caller and that of the call centre representative. By implementing **diarization,** it enables voices to be split and the caller's to be analyzed separately.

This is a key differentiator. To optimise storage, many call centres **store recorded voices on mono audio.**

Thales' biometric technologies

Thales has more than 200 biometric deployments in 80 countries, supporting strong biometric authentication and identification programmes for governments and businesses. Acquiring Cogent Systems enabled us to leap ahead in the field of trusted digital identities and build on Cogent's 27 years of biometric technology expertise. Our comprehensive suite of biometric verification solutions can be adapted to suit varying requirements for security and flexibility.

200
biometric deployments **in 80 countries**

Thales' core expertise: digital identity

At Thales, we work with some of the world's largest businesses and governments, providing flexible technological solutions that help meet the need for greater security and convenience simultaneously. Our technology serves as the basis for over 150 eGovernment programmes. Digital identity remains at the core of our expertise, as we enable hundreds of our partners to implement advanced authentication and security solutions.

450
MNO Customers

Serving as a trusted partner to MNOs over many years, we have supplied state-of-the-art products and services, compliant with the latest GSMA specifications. We provide SIM cards and manage services to more than 700 million subscribers and have already deployed more than 1000 solutions. Our products comply with the most demanding international standards, such as those defined by the U.S. Department of Commerce, the FBI, Interpol and the American National Standards Institute.

By merging our expertise in digital identity with long-standing partnerships with more than 450 MNOs, we seek to help operators provide the best possible experience to billions of people.

> Thalesgroup.com/Mobile <