VocalPassword™: voice biometrics authentication.

Friendly voice authentication across web, IVR, call center, or mobile.

NUANCE

VocalPassword™ for easy and secure authentication.

VocalPassword, the world's most widely deployed voice biometric solution, enables easy and secure authentication by analyzing a person's voice. Trusted by hundreds of organizations around the world to verify the identity of millions of individuals on a daily basis, VocalPassword delivers the most accurate, scalable and flexible voice biometric platform. Designed to serve as a unified authentication solution across your organization, VocalPassword can authenticate your customers as they access various self-service applications, such as a SmartPhone App, an IVR or a web portal.

VocalPassword can also serve to validate high-risk web and credit card transactions. Regardless of the application, users simply need to speak a passphrase such as "My voice is my password" to validate their identity.

Key benefits

– **Improve customer experience** – Transform the authentication process into a positive experience by eliminating the need to remember PINs, passwords or invasive security questions.
– **Improve self-service usage** – Improve the usage of your self-service customer care assets, such as SmartPhone apps and IVRs, by eliminating the failure rate caused by forgotten PINs and Passwords.
– **Enhance security** – Decrease fraud by verifying identity via an authentication factor that is unique to every individual instead of knowledge-based credentials than can be easily compromised.

New capabilities in V9

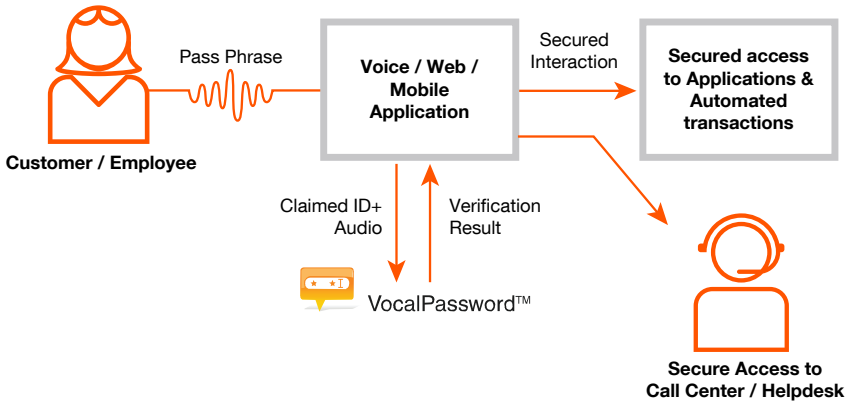
VocalPassword v9 brings a series of new innovations which are designed to enhance the customer experience while strengthening anti-fraud capabilities. These include:

– **Precision voice biometric engine** – Delivers up to a 50% improvement in accuracy over v8 VocalPassword performance.
– **SmartAdaptation** – Enables fully automated enhancement of voiceprints based on the analysis of failed authentication attempts by legitimate users.
– **Automated fraudster enrollment** – Prevents brute-force attacks by detecting and adding individuals to the fraudster list that attempt to access several accounts.

Identification and verification

Text-dependent biometric engine
Requires speaking a fixed passphrase such as “My Voice if my Password” or a set of digits such as a phone number.

– **Enrollment** – Enrollment is performed using three consecutive renderings of the selected passphrase. The passphrase can be in any language or accent and should contain at least 2 seconds of audio.
– **Verification** – VocalPassword verifies the speaker by comparing a single repetition of the enrolled passphrase to the voiceprint stored in the system’s voiceprint repository. Several repetitions of the speaker’s passphrase can be added and linked together to obtain a single score or decision.
– **Identification** – Speaker identification is carried out by comparing a single repetition of the speaker’s passphrase to a list of voiceprints owned by the speaker or multiple speakers.



Text-independent biometric engine
Operates on a live conversation.

– **Enrollment** – Text-independent enrollment is performed using samples of the speaker's unconstrained voice. While a voiceprint can be trained using a few seconds of voice, additional voice samples will provide a more robust voiceprint.
– **Verification** – Text-independent verification is performed by comparing a speaker's voice sample (unconstrained speech) to a voiceprint stored in the system's voiceprint repository.
– **Identification** – Speaker identification is carried out by comparing the speaker's voice sample to a list of voiceprints or a predefined group.

Text-prompted biometric engine
Random passphrase is used, typically a set of digits, letters or both.

– **Enrollment** – Enrollment is performed using three samples of the speaker's voice repeated in predetermined utterances containing the designated speech atoms. The enrollment phrases (or sequences) are provided by the system and are defined using a preconfigured dictionary. In order to allow for language and accent independency, the target speech atoms (defined as seeds) are predefined in the system. No ASR engine is required.
– **Verification** – Text-prompted verification is performed using a phrase that contains a randomized subset of the speech atoms provided during enrollment. The speaker repeats the phrase, and the system verifies the speaker by comparing the speaker's voice sample to the voiceprint stored in the system's voiceprint repository. The verification phrase is provided by the system to the application in real time based on a predefined verification dictionary.
– **Identification** – The calling application generates the prompt as in the verification process. The speaker repeats the phrase, and the system verifies the speaker by comparing the speaker's voice to a list of voiceprints owned by the speaker or multiple speakers.

"Voice biometrics is a unique identifier that will help us improve the customer experience," said Dominic Venturo, chief innovation officer for U.S. Bank Payment Services. "Exploring a spoken passphrase login through this technology is a logical next step."

usbank

Fraud prevention

Mitigating recording threats
The threat of fraudsters using voice recordings of legitimate speakers.

- **Liveness detection (Intra-session voice variation)** – This unique and patented method significantly reduces recording threats. Following text-dependent verification, this method uses text-independent voice biometrics technology to compare the voice sample captured during the text-dependent verification process, with an additional sample captured by prompting the speaker to repeat a random or semi-random sentence. By combining the obtained biometric scores and validating that the speaker indeed repeated the requested utterance (using VocalPassword's Utterance Validation engine or ASR), a liveness detection score is extracted.
- **Prompted passwords verification** – Prompted verification requires the user to repeat a random phrase that is a subset of speech atoms (digits/ words) trained during enrollment. Prompted verification provides protection against interception and playback attacks, as each session uses a different subset of the trained speech atoms.
- **Playback detection** – VocalPassword's patented playback detection algorithm runs as part of the verification process and identifies audio segments that unnaturally match audio segments that were previously used for verification/enrollment.

Detecting known fraudsters
Using watch-lists.

- **Fraudster detection** – Nuance's award-winning fraudster detection capability allows the system to keep track of known fraudsters. In a common passphrase scenario (i.e., "My voice is my password"), this functionality analyzes enrollment/ verification audio in real-time and alerts the application whenever a known fraudster is detected. Unique algorithms reduce the false alarm rate.
- **Automated Fraudster Enrollment** – Prevents brute-force attacks by detecting and adding individuals to the fraudster list that attempt to access several accounts.

Enrollment validation
Ensuring successful enrollment to achieve the best results.

- **Validating enrollment text** – VocalPassword guarantees that the spoken phrase is the correct phrase using one of two options:
- **Utterance Validation** – This is performed by VocalPassword using a proprietary algorithm. This algorithm is based on a background model that is trained as part of the system's setup (relevant when using common passphrase/s for enrollment/verification).
- **Automatic Speech Recognition** – Using Nuance Recognizer (NR9/NR10) as an optional add-on, VocalPassword evaluates the audio captured and checks that it contains the required text.
- **Enrollment consistency check** – This algorithmic functionality validates that multiple enrollment utterances are consistent with one another in terms of their content and biometric features.
- **Adaptation** – By using new audio to update existing voice templates, VocalPassword allows each speaker to maintain an accurate voiceprint according to changing background noises and voice tones that shift with age.
- **SmartAdaptation** – Enables fully automated enhancement of voiceprints based on the analysis of failed authentication attempts by legitimate users.

"Customers like the very simple and fast authentication process of only 5 seconds," said Fahri Arkan, assistant general manager of information technologies at Turkcell Global Bilgi.

TURKCELL

Using VocalPassword for knowledge-based authentication
As an additional authentication layer

– **Secret passphrases** – VocalPassword can be used for Knowledge-Based Verification by enrolling text-dependent voiceprints that contain the answers to verification questions.
– **ASR functionality** – VocalPassword's ASR add-on can be used to validate the speaker's answers. This requires the relevant language model and grammar to be in place.

VocalPassword flexibility
Customize VocalPassword to fit your needs

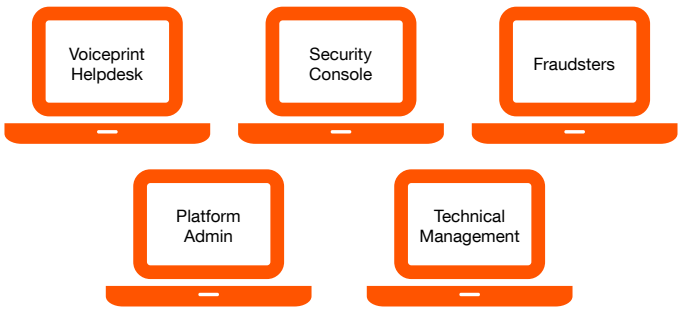
– **Multiple configurations and calibrations** – VocalPassword allows for use of multiple configurations and calibrations concurrently.
– **Decision mechanisms** – VocalPassword's built-in decision mechanisms may be overridden by ones designed by the customer through a custom plug in.
– **Multiple voiceprints per speaker** – VocalPassword allows for the enrolling of multiple voiceprints per speaker promoting security and language support.
– **Audio formats** – Besides built-in support for several standard telephony formats, any audio format can be supported through the audio format plug-in.

System architecture

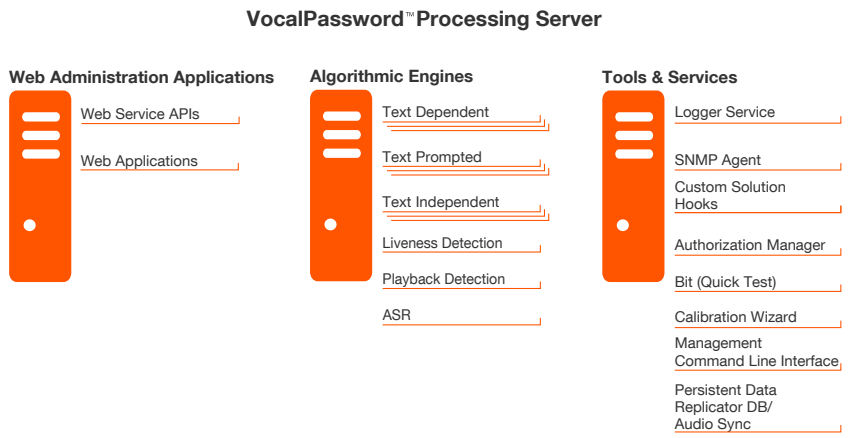
VocalPassword™ System Components

VocalPassword's main component is called the Processing Server. It hosts the speaker verification engines, which perform algorithmic processing, control client services, and acquire audio through API calls. Multiple servers can optionally be used in a redundancy scheme for high availability purposes or in a load-balancing scheme for scalability.

VocalPassword™ Web Systems



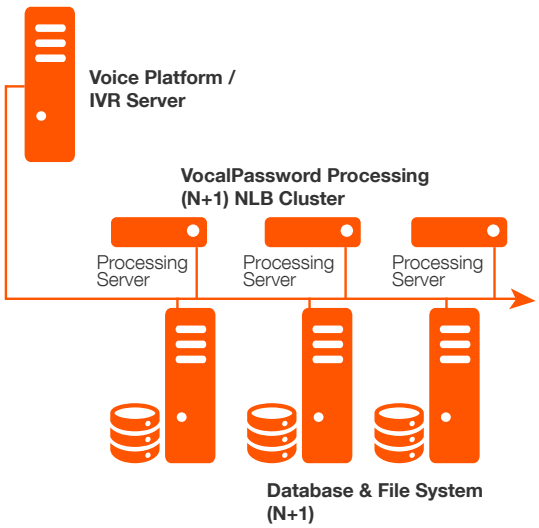
The Processing Server also hosts the Web applications used by system administrators, domain experts, helpdesk/contact center agents, etc. It is responsible for storing the system and voiceprint data in the database and file system. VocalPassword supports the use of N synchronized databases for high availability using a dedicated service (the PDR).



Deployment and integration

Scalability

VocalPassword scales up by utilizing multiple Processing Servers. The system's advanced Web service APIs enable client applications to work with any Processing Server. Scalability is achieved using standard load-balancing tools, such as Microsoft NLB clustering service and hardware-based network load-balancing solutions. Nuance VocalPassword was tested for stability and response times under extreme load conditions.



High availability

Nuance's products are designed to deliver constant, stable, and reliable service, securing customer-facing applications. Through the use of multiple Processing Servers and/or multiple databases, VocalPassword allows for a distributed architecture with no single point of failure, ensuring continuous service, 24/7. Configuration changes and voiceprint versioning mechanisms allow for system administration and upgrade with no disruption of service.

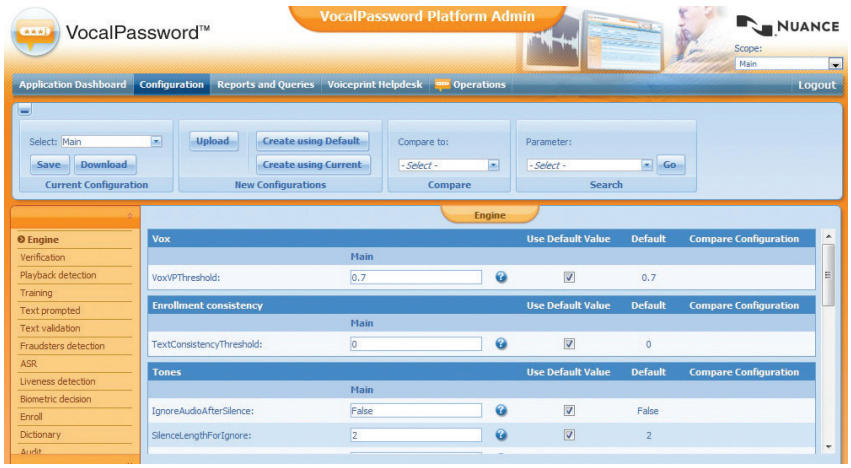
– **Database cluster** - VocalPassword can operate in a database cluster architecture. This architecture is usually implemented at a single site and provides high availability by using at least two databases and highly reliable hardware and networks.
– **Multiple data repositories** - Each VocalPassword Processing Server can work with n databases, optionally located in different sites. When the primary database is inaccessible, the Processing Server automatically switches to the secondary database in order to save the information. VocalPassword includes a real-time synchronization module that synchronizes n databases.

Multi-tenancy

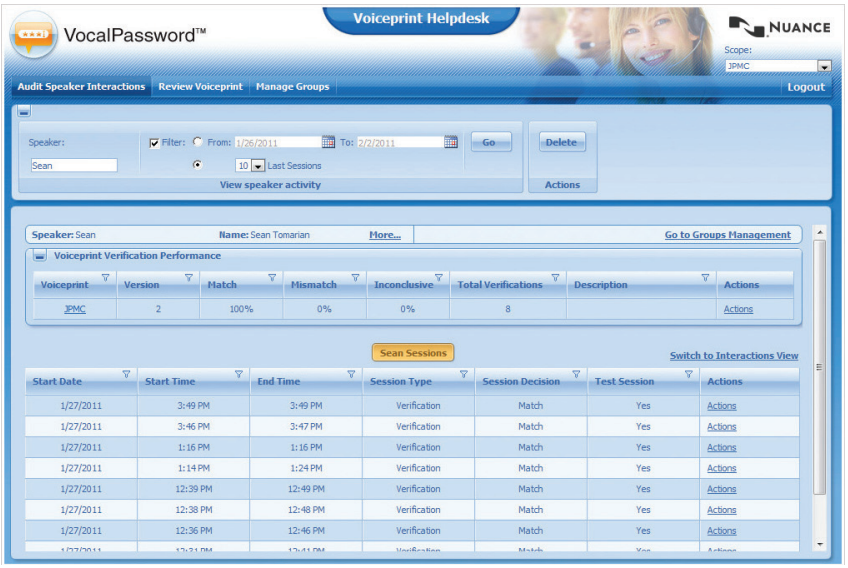
VocalPassword's multi-tenancy capability allows for the logical partitioning of the entire system in a secure and effortless manner through the use of scopes. This allows for a clear-cut separation of the system's data, configuration, audit, roles, etc., within an organization, enabling a single enterprise to use VocalPassword for multiple/distinct applications in different business units. Multi-tenancy is ideal for a hosted solution, enabling a service provider to offer VocalPassword as a service for multiple enterprises. Regardless of which system tool is used or what API method is executed, any operation is performed in the context of a specific scope. Scopes are assigned to users/customers by the system security administrator.

VocalPassword Web applications

– VocalPassword's Platform Admin is a Web-based application that provides a variety of tools for properly setting up the system and its biometric functionality as well as managing speakers, voiceprints, and groups. Users can utilize this application to configure VocalPassword, perform queries and reports, and monitor system usage.



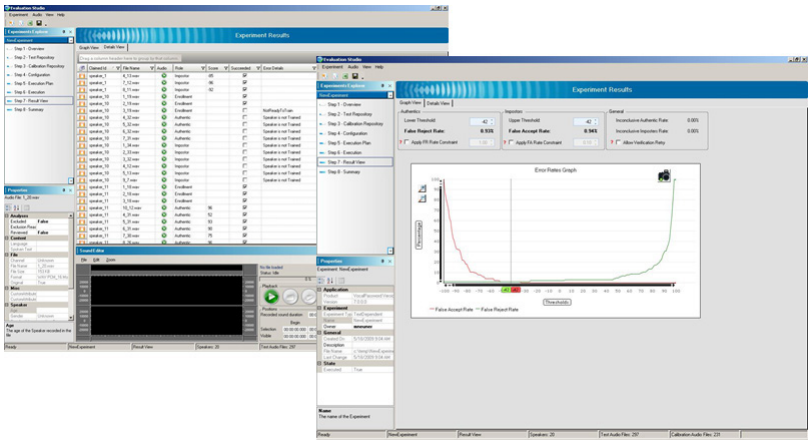
– VocalPassword's Voiceprint Helpdesk provides a set of tools allowing for auditing and reviewing of a speaker's interactions with the system. Users can utilize Helpdesk functions to audit verification results and decisions, edit speaker information, delete a speaker, edit a voiceprint, and more.



– VocalPassword's Technical Management is an application enabling technical personnel, who are in charge of the system's health, to monitor VocalPassword's system components' status, audit system-wide logs, schedule administrative tasks, such as audio purging, upload and view system licenses, and more.
– VocalPassword's Security Console is an application enabling security personnel to audit VocalPassword operations and analyze specific verification and identification processes. The application provides tools for managing fraudster's voiceprints and groups. In addition, Security Console collects and presents diversified security alerts.

– VocalPassword Fraudsters application supplies all the tools needed in order to perform real-time fraudster detection when identity theft is attempted. Use the application to manage fraudster and watchlist entities, analyze suspicious audio segments, and compare them to known fraudster voiceprints. An extensive reporting mechanism is available for audit purposes.

Evaluation Studio
Evaluation Studio is a revolutionary product that addresses the need to professionally plan, test, and analyze voice biometrics systems and technologies. Nuance Evaluation Studio is used for benchmarking different vendor's products, evaluating, piloting and rolling out a selected product, or just researching voice biometrics technology and its underlying performance.



– **VocalPassword Fraudsters** – Application supplies all the tools needed in order to perform real-time fraudster detection when identity theft is attempted. Use the application to manage fraudster and watchlist entities, analyze suspicious audio segments, and compare them to known fraudster voiceprints. An extensive reporting mechanism is available for audit purposes.

Technical Management Tools
– **QuickTest** – QuickTest is a simple application that invokes a predefined BIT (built-in-test), which includes a set of operations, simulating a complete voiceprint's life cycle.
– **SNMP Agent** – Each Processing Server has an SNMP agent service that handles SNMP get/set requests and sends SNMP traps when important system events occur. VocalPassword monitoring can be easily added to standard SNMP-based consoles.
– **MCLI (Management Command-Line Interface)** – MCLI is an extensive set of command-line based tools for immediate or batch system administration.
– **Calibration Wizard** – Calibration Wizard is a Windows application allowing for system calibration using customer-supplied audio files. Calibration is required for optimizing system accuracy.
– **Performance Counters** – VocalPassword utilizes Windows Performance Counters. These counters provide information as to how well the VocalPassword system is performing. The counter data can help determine system bottlenecks and fine-tune application performance."

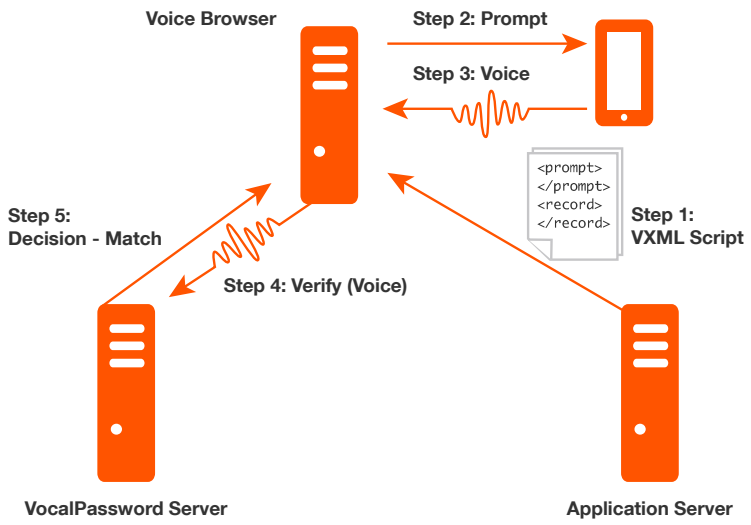
Interfaces
VocalPassword uses an enhanced, open, and flexible Web service API, ensuring smooth, platform-independent integration using any programming

"Call durations decreased about 15%, customer satisfaction increased 85% and worker satisfaction increased 97%," says Vodafone Turkey AGM Phil Patel, following deployment of VocalPassword."

vodafone

environment. The VocalPassword API is session aware, allowing users to associate multiple API calls with a single session and applying a session decision logic.

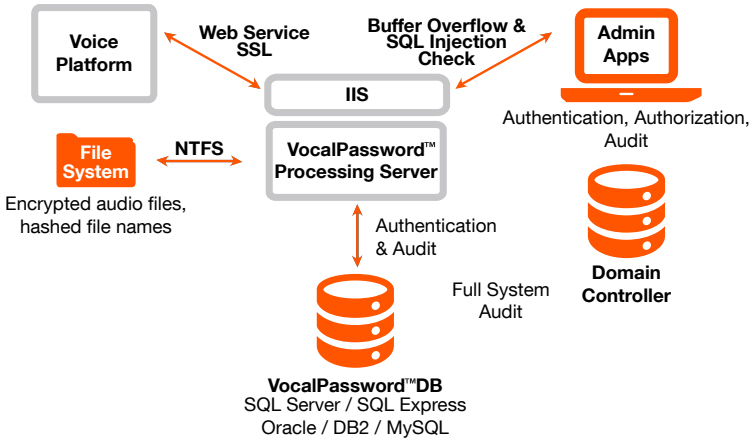
- **VocalPassword Server API** – VocalPassword's Server Web Service methods are used by client applications to perform operational functions, such as enrollment, verification, identification, and voiceprint administration. Enrollment and verification audio can be supplied to VocalPassword as part of an API call or provided as a URL to a previously recorded audio file. The API is fully compatible with VXML 2.0. Integration can be done directly from the VXML script, without passing through the application server.
- **VocalPassword Manager API** – VocalPassword Manager Web Service methods are used by the administration applications. The Manager API allows for system-level operations, such as changing configurations and uploading licenses.
- **VocalPassword Windows operations** – VocalPassword Windows operations enable users to send audio files to VocalPassword for processing in a straightforward manner. Available operations include Enrollment, Verification, and Identification. For example, a user can select three audio files containing a speaker's rendering of a passphrase from Windows Explorer, and create a voiceprint in VocalPassword by selecting the "Enroll" option under the VocalPassword item in the context menu. Alternatively, the user can select a folder containing hundreds of audio files and evaluate them against a stored voiceprint by initiating a "Verify" operation. Once an Explorer Extension operation is selected, a corresponding pop up message is displayed, prompting the user to enter required information. Operation status is reported back to the user as a message box in the Windows task bar. Verify and Identify operations generate a result file that can be processed by standard tools like Excel and Notepad.
- **VocalPassword Platform Integration with Voice XML Platforms** – VocalPassword has been successfully integrated with leading VoiceXML platforms using both VBScript and JavaScript. Integration with any VoiceXML platform can be easily accomplished using Nuance's sample code and VoiceXML scripts. VocalPassword natively supports calling its API using VXML data tag. Nuance is an active member of the VoiceXML SIV group and has contributed to the adoption of speaker verification functionality as part of VoiceXML 3.0.



Security features
VocalPassword's security design and features are based on the Common Criteria Protection Profile for biometric systems and has successfully passed third-party security audits performed by customers. VocalPassword ensures data and system protection by implementing the following security measures:

- **Role based authorization** – Access to system applications, resources, and services is governed by roles which can be customized to meet specific security needs.
- **Database access** – Database access is protected by integrated Windows security or by using an encrypted username and password mechanism.
- **PII & audio encryption** – personally identifiable information and Audio encryption is supported with VocalPassword's built-in encryption mechanism, as well as with HSM (hardware security module) and custom encryption mechanisms.
- **Voiceprint security** – Voiceprints are stored in a proprietary format in the system's directory and cannot be reverse engineered. Voiceprint IDs are signed using a unique key and cannot be used outside the system or in other VocalPassword systems.
- **Interface protection** – Access to the system service (API) is controlled using IIS6 or IIS7 security supporting SSL encryption All authentication schemes are supported: Integrated, Basic, Digest, and Certificates.
- **Audit and audit protection** – A full audit trail is stored in the system's database. All voiceprint usage and manipulation records are available and stored securely in the system.
- **Administration access control** – Administration and configuration applications utilize integrated security.
- **Input validation** – Input validation serves as protection against SQL injection, buffer overflow, and XSS attacks.

Intergrated Windows Security



Quality standard
VocalPassword is developed by Nuance Communications, under a quality system certified as complying with ISO 9001:2008 by the international Standards Institution.

Minimum requirements

Recommended Hardware	
Processor	2 X Quad Core CPU
Memory	4GB
Storage	20GB
Software	
Operating System	– Windows 2008 R2 – 64 bit Enterprise Edition & Standard Edition SP2 – Windows 7 – 64 bit Enterprise Edition & Professional Edition
Web Server	IIS7
Database	SQL Server 2005 & 2008, SQL Express, Oracle 11g with RAC support, DB2 9.5, MySQL 5.5
Browser	Explorer 8.0 and up, Mozilla Firefox 3.5 and up, Google Chrome 25.0 and up

Selected specification

Minimum VoicePrint Audio	2 seconds, 3 repetitions
Audio Format	8 bit Alaw, 8bit Ulaw, 8/16bit Linear, Custom (via CODEC plug-in)
VoicePrint Size	50K-100K
Management Protocol	SNMP V2
API	SOAP (XML/HTTP), HTTP (Get/Post)

About Nuance Voice Biometrics
Nuance is the global leader in voice biometric solutions, with over 30 million enrolled voiceprints and a global customer base that spans all major industries. Nuance has developed over the last 12 years unrivaled experience in delivering successful voice biometric solutions that enable organizations to improve customer satisfaction reduce costs and improve security.

For more information about Nuance's Voice Biometrics solutions, please visit our Web site at **Nuance Voice Biometrics**.

Awards
VocalPassword –
Best Implementation Awards

Speech Technology Magazine 2010 Implementation Award (Vodafone Turkey)

Speech Technology Magazine 2008 Implementation Award (Bell Canada)

About Nuance Communications, Inc.
Nuance Communications is reinventing the relationship between people and technology. Through its voice and language offerings, the company is creating a more human conversation with the many systems, devices, electronics, apps and services around us. Every day, millions of people and thousands of businesses experience Nuance through intelligent systems that can listen, understand, learn and adapt to your life and your work. For more information, please visit nuance.com.

NUAN–CS–2340–01–B, May 12 2014