validsoft

Using Voice Biometrics On-Device or Network-based Authentication?

A White Paper analyzing a FIDO based approach to the deployment of the Voice Biometrics.

The FIDO Alliance was formed in 2012 with the purpose of replacing passwords and their transmission over the Internet. Its on-device only model, however, fails to support today's Omni-channel business environments.

FIDO: The Original Purpose

The original FIDO premise of replacing passwords with PKI-based authentication, thus preventing the loss and theft of passwords through data breaches, as a rationale is not unreasonable. It was based on the assumption that the user would authenticate themselves to their device, using a variety of methods including passwords, and the device would then authenticate itself to the re uired web site using the device s stored private key.

With the adoption of biometric support to authenticate the user, the same rules had to be followed, i.e. the user authentication had to occur on the device, followed by the device authenticating to the website. The FIDO alliance claimed that an on-device biometric model was more secure than a server model because of potential data breaches. However, this ignores the fact that biometric models or templates, unlike passwords, are not shared secrets that can be used by anyone in possession. It also ignores the fact that biometric models are stored as encrypted digital representations of a physiological attribute that cannot be reengineered they do not store the physiological attribute. However, in an omni-channel world, the FIDO model of simply authenticating to a website or app is limited and does not address all challenges of password-dominant systems where device-based authentication cannot apply. Organisations wishing to adopt a biometric solution which they control and monitor are in fact excluded from deploying a FIDO-based solution.

Voice Biometrics offers a natural **high trust, low friction** experience.

The Benefits of the Network

Firstly, as organisations now support multiple channels of communication with customers, being able to provide a single, consistent approach to authentication is key. The only biometric modality capable of achieving this is voice, given the sheer volume of customer interactions that occur through contact centres, both agent driven and automated IVRs.

Further to this, AI provides the ability for customers to speak with Bots not only on these channels but also on the web and in mobile Apps. These are conversational channels that re uire the biometric authentication to occur within the channel. The FIDO model does not work on telephony channels or digital channels supporting person-to-person or person-to-Bot conversation. or can it provide continuous authentication, a re uirement for any voice activated commerce. It merely provides logon authentication.

Ubiquity, **digitisation** and **access** are driving the intelligent multi-channel experience omni-channel is a given.

Providing a PKI-based logon solution also ignores the fact that websites will transition away from static pages to include dynamic interactive services provided largely through interactive browser technology (WebRTC, HTML) and AI. Voice is the initiator of AI interactions and through that is also becoming the new UI of apps, smart speakers and websites.

Another ma or drawback of the FIDO model is the restrictive usability of the on-device model. Because the FIDO authenticator is resident on the device, the use of a different device to access a website is not allowed unless that device is registered with the site also and receives a separate private key. It would also then re uire a separate voice biometric enrollment. The same issue applies when a user purchases a replacement or complementary device such as a phone, tablet or computer. They must go through the registration and enrollment process all over again.

Any voice biometric solution must also cater for re-enrollments, re uired when an initial enrollment is not of sufficient uality for whatever reason. In a networked model this can be performed in a controlled and secure environment. In the FIDO model, if a voice enrollment is poor uality the user would be locked out of the corresponding website forever, so a back door must exist to create a new enrollment. Any back door is a weakness in the security model that can be exploited by someone with access to the device.

Financial services web sites such as Internet banking also re uire more than authentication. Due to well understood Man-in-the-Middle and Man-in-the-Browser attacks, financial transactions also re uire transaction verification (i.e. confirming the transaction details correspond to the users instructions and have not been intercepted and or tampered with). Voice biometric providers such as ValidSoft understand these re uirements and the capability is included within the overall voice biometric solution. Once again, FIDO provides authentication only, meaning banks and other service providers would need to deploy a secondary solution to protect transactions from these types of attacks.

Advanced voice biometric solutions also do more than ust authentication. One of the crucial functions voice biometrics play is real time processing of watch lists monitoring and comparing files containing the voice biometric models of known fraudsters etc. These are commonly used within financial services, where the voice of the person authenticating is compared to every model in the watch list in real time. However, in a FIDO model, the audio of the person accessing the website is not available to the bank, meaning no such watch list or other fraud-logic processing is possible.

Similarly, advanced solutions can also perform comparison processing, meaning every model enrolled in a database of users is compared to every other model in the database. The purpose of this is to detect potential duplications which could result from fake credentials and identities being used by bad actors. An example of this could be false bank accounts used for money laundering or fraudulent electronic transfers (Internet banking theft). Welfare agencies is another example, where fraudsters might set up false identities to claim welfare or social security payments under multiple guises.

Password authentication is completely different to biometric authentication and a solution such as FIDO, designed to protect against the weaknesses of the former, does not provide the wide-ranging and holistic benefits or capabilities of the latter. A customer-centric model with a central voice enrollment, accessed over any channel and on any device with a microphone, that provides seamless and continuous authentication and fully supports AI and speech commands is the optimal model of authentication and achievable only by voice biometrics.

Learn More

ValidSoft is a leading voice biometrics software company with a long history of innovation in voice authentication and biometrics. Our technology is built using active, passive, and continuous voice-based authentication, guaranteeing that the speaker is who they are, always. Our solutions help to eliminate call fraud and identity theft. ValidSoft s uroPriSe privacy seals ensure compliance with U DPR and other leading Data Protection and Data Privacy laws like HIPAA, Digital Identity uidelines, Vectors of Trust, Federal Identity Program uidelines, etc. ValidSoft is consistently recognized by third-party analyst firms as a market leader. See how ValidSoft is powering the Future of Identity at www.validsoft.com

Contact ValidSoft

UK Office:

Moorgate
London C R
United Kingdom

USA Office:

Pearl Street
Hartford, CT
United States of America

Email

re uest validsoft.com

Phone

( ) -

Confidentiality and Disclaimer

This document may contain references to information that has been obtained from sources believed to be reliable. ValidSoft does not guarantee the accuracy, completeness or ade uacy of such information, and shall have no liability for errors, omissions or inade uacies. The recipient assumes sole responsibility for the interpretation and use of this material for its intended results. Predictions and forward-looking statements in this document reflect current expectations concerning future events and are sub ect to risks and uncertainties, many of which are beyond the control of ValidSoft. ValidSoft undertakes no obligations to update these statements as a result of new information. Opinions expressed in this document are sub ect to change without notice.