EVA WEB

Add another layer to your multi-factor authentication suite and allow for a more secure and seamless experience when accessing systems and data.

EVA started in contact centers and is now available for web-based platforms. Organizations can integrate EVA Web into their system solutions to provide secure and frictionless voice-based identification and verification capabilities. This means that organizations can replace insecure and outdated security methods such as PINs and passwords and allow users to access online systems and data such as web portals and chatbots through a more seamless experience.

KEY CAPABILITIES

ACCESS ONLINE DATABASES AND SYSTEMS SECURELY

EVA Web enables people to securely verify their identity before accessing databases and systems online. EVA Web can be used as a single authentication option, eliminating device-based and knowledge-based (PINs and passwords) authentication processes.

More commonly, EVA Web is used to improve multi-factor authentication (MFA) processes combining device-based authentication with seamless voice biometric verification when accessing secure systems like chat, messaging and websites. Whilst having access to a trusted device like a laptop, smartphone or tablet provides some level of assurance that only authorized people can access services and data, devices can be compromised either physically or virtually by bad actors who gain control of the device.

MOST SECURE BIOMETRIC PRINT

Whilst fingerprint and facial recognition may provide some convenience in assuring identity, fingerprints and faceprints that are created and stored on the device are only as secure as device PINs that are used to create and change finger and face prints.

EVA Web adds a layer of security where the legitimate customer's voiceprint is created and stored within the client organization's secure infrastructure that controls access to systems and databases. With EVA Web, the client organization retains control of the voiceprint and can be assured that only legitimate customers will gain access to secure systems and databases.

SEAMLESS EXPERIENCE

EVA Web provides a more secure and convenient authentication process than outdated and intrusive methods such as requiring answers to personal identification questions like birth date or postcode.

When used on devices with a microphone, EVA Web enables people to access services with any device they have access to without needing to remember passwords or answers to secret questions. EVA Web also provides a more secure and convenient MFA than one-time passcodes (OTPs) which are sent via SMS, email, or separate hardware device like RSA tokens that many organizations use to enable secure transactions.

FRAUD PREVENTION AND PROTECTION

Fraud events can occur when a bad actor gains physical or virtual access to a trusted device and intercepts the OTP. EVA Web solves this problem by requiring the OTP to be spoken and the voice match is biometrically compared to a voiceprint stored in the authorizing enterprise's secure vault.

EVA has additional fraud prevention and detection benefits not available with device-based authentication. The audio collected during an enrollment or verification attempt can be compared with a list of known fraudsters enabling real-time fraud detection so immediate counteractions can be initiated.

INTEGRATION POINTS

EVA Web integrates with leading identity providers (IDP) platforms including Okta, PingFederate, Auth0 by using standard browser-based security technologies and protocols such as JWT, SAML, and OIDC.

AGAINST EXISTING SOLUTIONS

MULTIPLE VERIFICATION FACTORS

EVA Web is more secure and convenient because it provides several separate verification factors when a registered user verifies their identity.

The authorized person's voice must biometrically match the centrally stored voiceprint. This factor is device-independent as the process occurs using a voiceprint securely stored by the organization responsible for securing the data.

UNIQUE TRANSACTION

The person must say the digits that are uniquely created and displayed for each specific transaction. A transaction OTP is sent to the device the user is attempting to verify on. If the device is trusted by the IDP platform, then the device ID provides an additional factor. When the authorized person reads the correct OTP from the screen the process proves the authorized person read the OTP from the screen of the trusted device which provides a liveness test and non-repudiable digital signature.

In some scenarios, an additional knowledge-based question can be answered by the authorized voice to provide an additional factor. If the legitimate person knows the answer to "What is your account number/ phone number/ date of birth?" and their spoken answer matches the stored voiceprint as well as the correct answer, then this adds a knowledge based factor to the level of security.

Auraya does not recommend this knowledge-based approach for most scenarios as knowledge-based questions are often forgotten by legitimate users and whilst EVA protects against bad actors using a recorded voice to spoof the system, bad actors can attempt to record a person saying these knowledge-based questions and attempt to spoof the system by manipulating the recording.

DIALING OUT

For devices without a microphone, there is an option for EVA to dial out to a known and trusted phone number (adds a trusted device factor) or to dial out to a number provided by the user.

INTEROPERABILITY

EVA Web is completely interoperable with EVA for Amazon Connect and EVA Forensics. In addition, existing integrations with PingFederate, Auth0 and Okta allow administrators who use these platforms to select EVA as a factor and configure all the options necessary to activate EVA Web as an authorized factor. Administrators will also have access to the EVA Web management console to get information and relevant reporting data and any other controls necessary for EVA to be used by organizations. If your IAM platform has not yet been integrated with EVA Web, contact the team at Auraya for assistance.

AVAILABILITY

AWS MARKETPLACE

EVA Web capability is available on the AWS marketplace. Clients create EVA in their own AWS instance using an Amazon Machine Image (AMI). This means the client organization retains ownership and control over all voice biometric and audio data. AWS metering service calculates the number of transactions each hour and adds the usage charge to the client organizations monthly consumption fees. The end-user license agreement is the standard AWS EULA for this type of service.

PRIVATE OFFERS

For organizations looking to scale with EVA Web, Auraya offers a range of private offers where the price of a transaction can be negotiated for a combination of committed volume and or committed time. Auraya also provides private offer options for Amazon Connect Consulting partners and IAM platform providers so they can incorporate EVA for MFA functionality into their solutions.

SOLUTION TEMPLATES

EVA Web is also available as a solution template for resellers and end-users. The solution template allows consulting partners and end-users with EVA accredited technical teams to customize EVA for Web and integrate EVA Web with EVA for Amazon Connect and EVA Forensics.

Auraya Systems Pty. Ltd.
Auraya is a voice intelligence company with the mission of empowering people and organizations to interact and engage with convenience and security in all channels and languages. Auraya develops next-gen voice biometric AI technology to deliver easy-to-use and highly secure speaker recognition and fraud detection capabilities. Auraya provides its technology to a global network of partners who incorporate Auraya's voice biometric technology into their secure, customer-facing applications and fraud detection solutions. The ecosystem of partners delivers solutions in all industries including government, education, healthcare, financial services, retail services, and telecommunications. If you would like to talk to the team at Auraya, send us an email at info@aurayasystems.com.