PARTNER CASE STUDY

Jumio Trusted Identity Platform, 2019

Identity Verification with ZoOm® 3D Face Authentication

At a Glance

Jumio Requirements

- Liveness Detection for Onboarding
- Authorized user re-verification for future account access
- Universal mobile smart device and webcam support
- Intuitive, user-friendly interface
- Straightforward implementation and management

Solution

Outperforming all other login solutions, including password, PIN and other biometrics, FaceTec's NIST/iBeta -certified, 100% software, 3D Face authentication, ZoOm, met or exceeded all Jumio's customer authentication process requirements on mobile devices and PC's with webcams. ZoOm has been rigorously tested by Jumio's security team and by internationally-recognized, sanctioned 3rd-party testing organizations. Liveness Detection is recognized as the most critical component of an unsupervised user verification.

Overview

Jumio, based in Palo Alto, CA, with offices in Europe, South America and the Asia Pacific, is considered the most accurate identity verification solution in the market by a large margin. Jumio's solutions are used globally by leading companies in financial services, the sharing economy, retail, travel, crypto-currency and online gaming. Jumio has also received numerous innovation and design awards, and has recently announced Jumio Authentication, a service that unlocks identities with secure 3D selfie technology.

Jumio has verified over 170 million identities, firmly establishing it as the global leader in Trusted Identity as a Service, combining ID Verification, Identity Verification and Document Verification for a complete solution to establishing the real-world identity of consumers. Leveraging advanced technology, including biometric face authentication, machine learning and human verification experts, Jumio helps businesses meet regulatory compliance in KYC and AML, reduce fraud, and provide a safe, secure and seamless customer experience.

To safeguard the highly sensitive and confidential information inherent in ID access and management (IAM), a truly secure access method must meet the following criteria:

- Ensure the person requesting access is verified as the authorized user *and* - to prevent spoofing – verify they are alive and present *at the time of account login*
- Be fast, and easy and intuitive enough for anyone to use daily
- Perform in a broad range of physical environments and circumstances
- Work for all users of standard smart devices and webcams
- Be simple for customers to integrate and manage

After rigorous internal testing, the ZoOm® 3D Face Login solution met or exceeded demanding usability and security requirements when tested in a wide variety of common environmental and situational circumstances with a diverse user base.

The Business Problem

IAM is expected to grow to nearly $15B by 2023 with a CAGR of 12%. Several driving factors for the increase in usage include a rise in security concerns from possible unintended use, damage and theft, heightened user expectations, compliance mandates and continued global increases in mobile access. To mitigate concerns that can arise in Jumio's use cases – including KBA replacement, fraud detection, KYC & AML, user re-verification, onboarding and high-risk transactions – user authentication safeguards must be in place to ensure that only a fully-vetted, authorized person is being given access to any given service.

It was also important for Jumio to find a single biometric that could be used during both the identity-proofing/verification stage, and subsequent, ongoing authentication.

In addition, costs and the user and business experiences must clearly benefit from effective authentication solutions, providing clear, positive impact on a company's image and bottom line. Authenticating a user – verifying they are the correct user, and present *in person* at the time of the login request – is a key requirement.

Choosing the Authenticator

Jumio considered and tested numerous purported face authenticators from many vendors, and many claimed they had capable liveness detection, including a solution that flashed random colors at the user's face. By the end of their testing, the choice was clear.

"

ZoOm quickly distinguished itself as the segment leader. In addition to its anti-spoofing detection capabilities, FaceTec's liveness detection offers some very tangible benefits in terms of a more streamlined user experience and omnichannel support.

"

-- Robert Prigge, President, Jumio

Assessing 2D Facial Recognition: Two-dimensional facial recognition can be very effective at matching the face a device's camera sees to a previously stored photo taken at a similar angle in similar lighting conditions, and it is a necessary first-step in making a positive ID. However, 2D face matching cannot distinguish between a photo or video spoof and a real, live person. Without robust Liveness Detection or 3D depth detection, it is not possible to anchor a human identity to a digital verification process. Presentation attacks would be far too easy to execute for the face modality to be considered secure enough for the Authentication solution. Some 2D face matchers try to add security by requiring the user to blink, wink or nod their head randomly. This may seem like it could prevent an inanimate spoof from accessing the system, but they are easily fooled by, for example, "Photoshopping" eyelids on a copy of the photo and toggling between the two. Further, 2D photos can even be made to smile, talk, nod and look around using simple avatar programs like CrazyTalk.

Assessing 3D Face Authentication: A 3D face biometric contains at least 100-times more data than a 2D photo or even video and can verify both identity and three-dimensionality using the same data. Some 3D face authentication methods are proprietary-hardware-based, and some require several seconds to authenticate. Intense, direct lighting can also overwhelm smart device cameras regardless of how good they are, preventing authentication.

There are two 3D face authentication approaches, hardware-based and software-based. Hardware-based three-dimensional face authentication is accomplished using specialized cameras, and expensive AI chips, sensor arrays and IR dot projectors that beam invisible dots onto a user to model a 3D face. While this approach can be effective in discerning three-dimensional from two-dimensional objects, there is one key issue: they lack actual liveness detection. A 3D object is not necessarily a real person. Dolls, masks, 3D prints and wax figures are all 3D but are not alive, and every 3D face sensing hardware solution that has been released can be fooled by at least one of these types of artifacts.

The ZoOm 3D face authentication software measures perspective distortion to prove the user's face is 3D and measures another 50 uniquely human traits. ZoOm converts a two-second video selfie into a proprietary biometric 3D FaceMap that contains all the necessary data to make an accurate face-matching decision *and* a highly trusted liveness decision. AI-driven continuous learning makes ZoOm even more effective over time, and developers at FaceTec are continually updating the algorithms to guard against any newly identified threats. ZoOm's FaceMaps are encrypted and securely stored in the cloud, which allows Users to authenticate across various operating systems and on multiple devices, making it ideal for large scale deployments.

Jumio announced their first end-to-end biometric verification solution, Jumio Authentication, coupling identity proofing with ongoing 3D Face Authentication powered by ZoOm

The Jumio Authentication Solution

Biometric-based Jumio Authentication establishes the digital identities of your users through the simple act of taking a selfie. Advanced 3D face map technology quickly and securely authenticates users and unlocks their digital identities.

The Authentication process performs the following steps:

- *Acquire*: When a new online account is created, Jumio captures an image of a valid government-issued ID (e.g., driver's license, passport or ID card) and a 3D face map.
- *Compare*: A high-resolution selfie is compared to the photo on the ID to reliably establish the digital identity of the new user.
- *Authenticate*: When future user authentication is needed, Jumio Authentication captures a fresh 3D face map and compares it to the original face map to unlock the user's digital identity in seconds.

In addition to providing these services and providing a seamless user experience, the verification process must also catch fake IDs, meet compliance mandates and work across a wide range of operating systems and device hardware.

facetec

FaceTec's patented, NIST/NVLAP iBeta-certified 3D face authentication software increases security and convenience with the most secure and intuitive biometric on the market. Now available for all smart devices and webcam-enabled systems, ZoOm leverages decades of Computer Vision and Artificial Intelligence experience to ensure positive identification, three-dimensionality and human liveness.

ZoOm is trusted to reduce fraud and theft by organizations of all sizes on five continents in banking, government, IAM, transportation and more.

Given the underlying complexity and the inherent importance of verifying identities digitally around the world in real-time, it is imperative the method used to authenticate the correct user can ensure that the correct user is present in person and in possession of the ID document.

The Biometric Authentication Technology Selected

FaceTec's ZoOm 3D Face Authentication exceeded the security and usability requirements for Jumio's customers' use cases. ZoOm ensured the onboarding experience allowed real users through easily but blocked spoof attacks that would allow fake account creation:

- ZoOm is Level-1 & 2-certified against presentation attacks
- ZoOm matched 3D face images with extreme accuracy
- ZoOm used standard 2D device cameras and webcams to create encrypted 3D FaceMaps on all modern Android and iOS smart devices and webcam-enabled systems (omnichannel support)
- ZoOm enrolled users consistently and reliably
- Enrollment took only 10-15 total seconds

ZoOm provided a re-verification option for Jumio:

1. After a user has onboarded with ZoOm and competed the Jumio's identity verification process, the user can return to authenticate at any time and re-verify themselves without having to scan their ID document again. They only must "ZoOm in" to prove their identity and liveness, gaining access to their account.
2. ZoOm also provides the ability for Jumio's customers to go password-free and use ZoOm to allow their users to quickly and easily login several times, every day.

Recommendations

When deciding on a biometric authenticator, security, usability, cost and future flexibility must be evaluated together.

1. *Security*: Unauthorized account or document access can be dangerous and costly, requiring strong security measures. For true user authentication, the method must accomplish four things during login:

    1) Verify human liveness traits
    2) Verify three-dimensionality
    3) Match images captured by the device to enrolled users' FaceMaps
    4) Encrypt unique 3D FaceMap data for secure storage and transmission

For the application to avoid spoofs by non-human representations of the authorized user (photos, videos, image projections, masks, etc.), the steps listed above must happen concurrently. Other face biometrics tested met one or two of the four required authentication attributes. ZoOm handled all four steps seamlessly and consistently.

An important note: All biometric solutions *must* be 3rd-party certified by a sanctioned lab to verify the performance claims made by the vendor.

2. *Usability*: User authentication will occur in a wide variety of circumstances and environments, and the experience needs to be consistent, fast and reliable. Authentication processes that take more than a few seconds, require special hardware, or are not easily accessible in inclement weather will be quickly rejected by typical users. The interface must be quick, and easy to understand and access. ZoOm's fast, simple selfie interface proved easy to use, even for the least tech savvy.

For more information about FaceTec and how ZoOm can solve your toughest authentication problems, please visit ZoOmLogin.com.

For business inquiries, please contact Rich Lobovsky at rich.lobovsky@facetec.com.

For press inquiries please contact John Wojewidka at johnw@facetec.com.

For the latest company and industry news and announcements, please visit FaceTec and Jumio

Usability must be considered for IT management, as well. ZoOm can perform user authentication without IT intervention: a liveness determination allows or blocks account access and ZoOm sends a pass-fail decision to the customer application. No additional processing is required, except when an organization requires other authentication steps, such as document verification.

3. *Total Cost*: Overall costs must include all direct and indirect expenses, as well as any projected savings from reductions in support overhead, breach mitigations and brand-damage repair.

Use licenses, subscriptions, in-house development or outright purchase costs are just the beginning of a realistic cost assessment. Technology support requirements must be considered, such as server setup and maintenance, additional hardware, additional personnel, coding and interface customization, periodic vendor support agreements, upgrades, bug fixes and internal customer support representatives.

A secure solution also offsets significant costs by preventing breaches, avoiding internal IT and post-breach mitigation costs, and preventing brand damage.

4. *Future Flexibility*: In the current environment, security technology and developing threats change rapidly. It is of strategic importance to select a security solution that is constantly improved and third-party tested. Updates must be developed and deployed quickly, and the solution must be able to react rapidly to market needs. It must also be cross-platform compatible, and able to work on any popular mobile or stationary device, even devices the user does not own. An AI-driven, 100% software solution is the only real-world approach to meeting all these demands.

Summary

By anchoring a user's human identity to their digital identity through robust liveness detection, Jumio can now provide ZoOm to their 500-plus customers, allowing them to securely create new accounts and access them from apps and web pages in a wide variety of circumstances. In the demanding world of digital identify where fraud is constantly attempted, yet users cannot be inconvenienced or turned away due to usability issues, ZoOm was considered the perfect login security solution for Jumio's globally-deployed verification and authentication services. Every aspect of ZoOm, from security to usability to costs, reinforced the solution as the best cross-platform biometric access method, exceeding Jumio's customers' expectations and requirements.

- *Security*: Seamlessly and consistently allows fast enrollment and authentication of real, registered users with valid IDs while rejecting fraudsters
- *Usability*: Fast and simple for users, works in nearly all lighting conditions, no special hardware required; quickly deploys for POC trials with easy app SDK integration, plus extensive visual customization options
- *Total Cost*: Insignificant integration costs, near-zero management/maintenance costs, straightforward per-user or per-session pricing, dramatically reduced password-reset related costs, increased usage and customer loyalty
- *Future flexibility*: Fast, seamless, timely updates; quick, thoroughly tested deployments; future-threat and customer-integration-needs ready