CASE STUDY

Turbi Carsharing Service, Brazil, 2018

Secure Driver Authentication for Vehicle Entry with ZoOm® 3D Biometric Login

facetec

TURBI
CAR ON DEMAND

At a Glance

Turbi Requirements

- Authorized driver authentication for vehicle entry for a fast-growing fleet of shared cars
- Universal mobile smart device support
- Intuitive, user-friendly graphical interface
- IT-friendly implementation

Solution

Outperforming all other secure login solutions, including password, PIN and other biometrics, FaceTec's 100% software, 3D biometric login, ZoOm, met or exceeded all Turbi's mobile customer authentication process requirements. ZoOm was fully integrated and operational within three weeks and now authenticates thousands of Turbi customers every month using ZoOm as the only login method.

Overview

The Turbi carsharing service launched in São Paulo, Brazil in 2017 as a major participant in the so-called Gig Economy, a collection of businesses that replace ownership or long-term associations with "gigs", or short-term, temporary experiences. Gig Economy businesses leverage inventories of products or services by acting as a single point of access and management for and by consumers.

Turbi is an ideal example of a Gig business; a convenient alternative to vehicle ownership with consumer access to a distributed fleet of on-demand vehicles used for short periods of time, primarily managed through a mobile app. However, to prevent fraudulent use or theft of conveniently available vehicles, a secure access method must meet the following criteria:

- Ensure the person requesting access is verified as the authorized driver and - to prevent spoofing – verify they are alive and present *at the time of vehicle pickup*
- Be fast and very easy for anyone to use
- Perform in a broad range of physical environments and circumstances
- Work for all users of smart devices with standard hardware and operating systems
- Be simple for IT to integrate and manage

After thorough internal testing, the ZoOm® 3D Mobile Face Login solution met or exceeded demanding consumer-level requirements an authorized driver is expected to encounter in a wide variety of typical environmental circumstances.

Business Problem

Carsharing, ridesharing and car hailing services are experiencing rapid global expansion, with year-over-year gains expected to be over 34% through 2022. But with the convenience of these popular connected services comes new worries about fraud and customer safety. To mitigate concerns like unintended use, damage and theft, user authentication safeguards must be in place to be certain that only a fully vetted, authorized person is using the service.

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 driver – verifying they are the correct user, and actually present *and alive* at the time of the login request - is a key requirement.

Choosing the Authenticator

Turbi considered and tested several access methods, including password, fingerprint, voice, eye scans, 2D face recognition and 3D face authentication.

Password: Easy to initially create, relatively simple to use and eminently portable, passwords were rejected because they are also very easy to share or phish. According to an annual security report by Verizon, 82% of all breaches involve compromised passwords.

Fingerprint: Fingerprint is easy to use and cannot be forgotten, easily shared or phished. However, a hardware fingerprint sensor is required in or connected to the user's device and they do not work well if the sensor or finger is dirty. Fingerprint sensors in mobile devices can be spoofed relatively easily using a photo or a "lift" taken. There are also usability issues for people with worn fingerprints, such as senior citizens, artisans and people who engage in daily physical labor.

Voice: Voice is not an appropriate application for this use case. Ambient noise is nearly always present, and an audible code could easily be recorded and reused for access.

"

Turbi's carsharing service is built on convenience, dependability, value and safety. To keep the experience safe from the start, we chose ZoOm to ensure only the right person has access to the right vehicle. We deployed our Turbi mobile app integrated with ZoOm in only a short three weeks from our very first conversation with FaceTec. The unmatched security, speed, simplicity and ease of management allow us to focus on growing our business. As we continue to add cars and customers, having a high level of security in place is a great comfort.

"

-- Diego Lira, CEO, Turbi

Eye scans: Retina and iris scans can be very secure. However, they require special hardware, do not work well in bright light and require the sensor to be uncomfortably close to the eye. The specialized hardware requirement made eye scans a non-starter.

2D Facial Recognition: Two-dimensional facial recognition can be very effective at matching the face a camera sees with a stored image from a previous enrollment, but it cannot distinguish between a photo or video spoof and a real, live person, making presentation attacks far too easy to execute for the modality to be considered secure. Ambient lighting can also be an issue.

3D Face Authentication: Three-dimensional face/head authentication (not just facial recognition) converts a video feed into a biometric FaceMap. A face biometric contains more data than photos or 2D video and can verify both identity and three-dimensionality using the same data. Some 3D face authentication methods are proprietary-hardware-based and do not verify liveness, and some require several seconds to authenticate, asking users to nod or smile (not a true liveness indicator). Intense, direct lighting can also overwhelm smart device cameras regardless of how good the software is, preventing authentication.

The Solution Chosen

ZoOm 3D face authentication from FaceTec met the security and wide-ranging, consumer-level usability needs for secure vehicle access. ZoOm ensured the experience was safe from account breaches that could compromise confidential accounts, or create opportunities for unauthorized users to gain vehicle control:

- ZoOm could not be spoofed
- ZoOm matched images with extreme accuracy
- ZoOm used standard 2D mobile device cameras to create encrypted 3D facemaps, for immediate use on all modern Android and iOS smart devices
- ZoOm enrolled and authenticated drivers consistently and reliably regardless of environment
- Enrollment took only 15-30 seconds and authentication took 1-2 seconds, well within consumer expectations

Secure login is simple and quick, with only two major steps:

1. Enroll (15-30 seconds): A new customer enrolls with ZoOm integrated into the Turbi vehicle access app to later authenticate at vehicle pickup.
2. Authenticate (1-2 seconds): The driver approaches the vehicle and uses the app to log in and authenticate, immediately unlocking the door for operation.

Recommendations

Before considering deployment, security, usability, IT manageability and overall cost must all be evaluated in both structured in-lab tests and a real-world proof-of-concept trial.

1. *Security*: A vehicle operated by an unauthorized person can be dangerous and costly, requiring a very high level of security for vehicle entry. For true driver authentication, it must do three things during login:

    1) match images captured by the device to the enrolled user facemap
    2) verify three-dimensionality
    3) verify human liveness

    For the application to avoid being spoofed by non-human reproductions of the user (photos, videos, image projections, masks, etc.), the three steps listed above must

FaceTec's patented human authentication software increases security and convenience with the most secure and intuitive 3D face biometric on the market. Now universally available for all smart mobile devices and webcams, ZoOm leverages decades of Computer Vision, Artificial Intelligence-Machine Learning experience to ensure positive identification, image three-dimensionality and human liveness.

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

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

For business inquiries, please contact Satya Yenigalla at Satya@FaceTec.com.

For press inquiries please contact John Wojewidka at JohnW@FaceTec.com.

happen concurrently. Other biometric options met one or two of the three required authentication attributes. ZoOm handled all three steps seamlessly and consistently.

2. *Usability*: Driver 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 work quickly, and be easy to understand and to access at all times. ZoOm's fast, simple selfie interface proved easy to use, even for the least tech savvy.

3. *IT Management*: Without IT intervention, ZoOm can perform user authentication entirely on the device, or match to a facemap stored on a remote server. In either case, a pass-fail token and a liveness confidence score is provided to the app allowing or blocking account access. No additional processing is required, except when an organization requires other authentication steps, such as document verification.

4. *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 also be assessed, such as server setup and maintenance, additional in-house or user hardware, additional personnel, custom coding and interface customization, periodic vendor support agreements, upgrades, bug fixes and internal customer support representatives.

Offsetting costs, a reduction in breaches afforded by a secure, easy-to-use solution will lower internal IT and post-breach mitigation costs, preventing expensive brand damage. Software-based solutions that operate on any existing smart device, and process and securely store data exclusively or primarily on the device, are the most cost-effective.

Summary

Today, thousands of Turbi customers use ZoOm to securely and immediately access their rented vehicles in a broad range of environmental circumstances using only their faces to authenticate and unlock the door. In the demanding, consumer-level use case of Turbi's vehicle access app, every aspect of using ZoOm as a secure, mobile biometric entry method met or exceed expectations and requirements within Turbi and for their customers.

- *Effectiveness*: Very high level of authorized driver authentication certainty, and user biometrics *cannot be shared or phished*
- *Integration*: A simple 2-3-hour app integration, the option to extensively customize look-and-feel, and the ability to quickly deploy for POC trials and production
- *Management*: Immediately available SDK and all supporting integration and customization documentation, no server configurations or costs, hands-off operation focused only on authentication
- *User Experience*: Simple selfie-style user interface, fast enrollment and authentication, works in nearly all environments and circumstances, no special user hardware or additional costs required, minimal environment adaptation required
- *Costs*: No additional servers or hardware, no additional IT support, reduced breach-related costs expected, very low cost/user subscription