CASE STUDY

MKB Bank, Hungary, 2017

Secure mobile customer account authentication with ZoOm® 3D Face Login

facetec

At a Glance

MKB Bank Requirements

- Authorized customer authentication for mobile account access
- Universal mobile smart device support
- Intuitive, user-friendly interface
- IT-friendly implementation
- Audit trail function for positive user verification

Solution

Outperforming all other biometric solutions, FaceTec's 100% software, 3D biometric login, ZoOm, met or exceeded all MKB's mobile banking customer authentication process requirements. ZoOm is being considered for several other W.UP secure authentication implementations

Overview

MKB Bank is Hungary's fourth-largest bank, and one of the country's most innovative. Fully aware of the gravity of growing digital fraud, MKB took a lead in mobile banking innovation in partnership with their IT services partner, W.UP, to ensure the highest level of account protection to prevent potential customer asset and data theft. The secure mobile banking account access method was required to meet the following criteria:

- Ensure the person requesting access is actually authorized and - to prevent spoofing and phishing attacks - they are alive and present *at login*
- Be fast and very easy to use any level of customer comfort
- Work for all users of smart devices with standard hardware and operating systems
- Perform in a broad range of physical environments and circumstances
- Be simple for IT to integrate and manage
- Provide an audit feature to more accurately assess fraud claims

After intense anti-spoofing testing and a successful proof-of-concept (POC) trial, ZoOm® 3D Mobile Face Login met or exceeded demanding consumer-level requirements a banking customer is expected to encounter in a wide variety of typical operational circumstances.

Business Problem

Juniper Research anticipates the number of global mobile banking users will overtake non-online users in 2018, two years earlier than anticipated. About two billion people are expected to access retail banking services with smartphones and other digital devices; a full 10% increase from 2017.

However, increased mobile use also increases exposure to fraud and account breach potential. While mobile banking improves usability and lowers costs, fraud concerns are hindering further adoption. According to a recent Federal Reserve Board survey, 73% of non-mobile banking customers pointed to security concerns as a reason for not banking on mobile. An IBM study (2016 Mobile Security & Business Transformation) found 58% of security experts at financial institutions ranked security concerns as a top risk, inhibiting banks from fully deploying mobile services.

Further complicating full mobile adoption is a marked increase in mobile malware and phishing schemes where, ultimately, the responsibility for assessing the validity of an "official" email falls on users themselves. As they become more sophisticated, and as mobile users have less time to make critical assessments, these attacks become increasingly more harmful.

Choosing the Authenticator

MKB Bank's IT integration partner W.UP considered several access methods, including password, fingerprint, voice, eye scans, 2D face recognition and 3D face authentication.

Password: Easy to create, relatively simple to use and eminently portable, passwords were rejected because they are very easy to share or phish. According to a 2017 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 and does 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 "lifted" impression. There are usability issues for people with weak or worn-down fingerprints, such as senior citizens, artisans and people who engage in daily physical labor.

"

MKB Bank has provided commercial services for the people and businesses of Hungary for more than 65 years. Our reputation was built on providing the very best services to our customers, including, today, the most secure mobile account access possible. ZoOm's unparalleled anti-spoofing liveness, depth detection and ease of use has translated into very quick user adoption and increased trust in our mobile products.

"

-- Mark Heténi, MKB's Deputy Chief Executive Officer

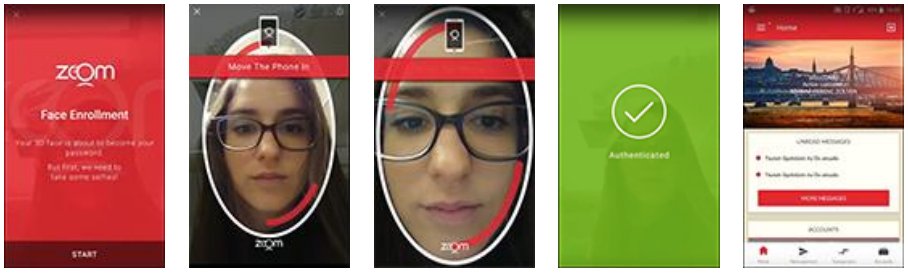
Voice: Voice is not an appropriate application for this use case. Ambient noise is nearly always present and an audible code could easily be recorded and reused for access.

Eye scans: Retina or 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.

2D Facial Recognition: 2D facial recognition can be very effective at matching what a camera sees with a stored enrollment image, but cannot separte a photo or video spoof and a live person, making presentation attacks too easy to execute. Lighting can also be problematic.

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

The Solution Chosen



ZoOm 3D Face Login from FaceTec met the demanding security and consumer-level usability needs for daily account access ensuring the experience was safe from breaches:

- ZoOm demonstrated a very high degree of image matching accuracy
- ZoOm used standard 2D mobile device cameras to create encrypted 3D face maps, allowing immediate use on all modern Android and iOS smart devices
- ZoOm enrolled and authenticated bank customers consistently and reliably
- Enrollment took only 15-30 seconds and authentication took 1-2 seconds, well within the acceptable timeframe
- ZoOm biometric data is ultra-secure and cannot be phished or borrowed, and is unspoofable against 2D images and video

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

1. Enroll (15-30 seconds): A new customer enrolled with ZoOm integrated into the access app so they could be later authenticated when requiring account access.
2. Authenticate (1-2 seconds): The customer opens the app, chooses to authenticate and is immediately granted account access for any transaction engagement.

Recommendations

Before 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 breach customer account can be very costly, requiring a very high level of security during login. For true authentication, it must do three things:

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

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 unparalleled 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 media inquiries please contact John Wojewidka at JohnW@FaceTec.com.

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 happen concurrently. Other biometric options met one or two of the three required authentication attributes. ZoOm executed all three seamlessly.

2. *Usability*: Customer authentication will occur in a wide variety of circumstances and environments and 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 rejected by typical users. The interface must work quickly, and be easy to understand and to access at all times. ZoOm's simple selfie interface proved easy to use, even for technology neophytes.

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 true cost assessment. Technology support requirements must also be assessed, such as server setup and maintenance, additional in-house or user hardware, additional IT personnel, custom coding and interface customization, vendor support agreements, upgrades, bug fixes and additional customer support representatives.

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

Summary

Today, with thousands of MKB Bank account authentication sessions every month, every aspect of using ZoOm as a secure, mobile biometric access method have met or exceed expectations and requirements.

- *Integration*: A simple 2-3-hour app integration and 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-related hardware or additional costs, minimal environmental adaptation required
- *Effectiveness*: The highest level of banking customer authentication certainty
- *Costs*: No additional servers or hardware, no additional IT support, reduced breach-related costs expected, very low cost/user subscription