CASE STUDY

KZen Networks, Tel Aviv, 2020

Cryptocurrency wallet user authentication and biometric backup

At a Glance

Technology Need

Biometric Account Recovery

Requirements

- Certified Liveness Detection
- Universal device support
- User-friendly interface
- Straightforward integration
- Ongoing monitoring & updates

Solution

Outperforming all other secure authentication solutions, FaceTec's NIST/iBeta-certified, 100% software, 3D Face Authentication solution, met or exceeded all KZen's user re-authentication process requirements on mobile devices and PC's with webcams. FaceTec 3D Face Authentication has been rigorously tested by KZen's security team who also performed multiple security audits on the implementation of the architecture. Robust, Certified Liveness Detection was recognized as the most critical component of an unsupervised user re-verification process enabling biometric account recovery.

Overview

KZen Networks, the Tel Aviv-based developer of the ZenGo crypto wallet, decided from the start to make the "perfect" cryptocurrency management solution. Their technology has been called a game changer and a revolution in crypto storage that can bring bitcoin, etherium and many other digital assets to the masses.

KZen knew that for mass adoption the next generation crypto wallets had to be trusted as more than just vaults to store an asset, and they needed to address the significant problem of lost or stolen keys. The news is filled with stories of missing or damaged hard drives containing the only method users could employ to access their wallets again.

KZen's definition of a what a successful crypto wallet should be must include the following:

1. Prime security and security
2. Diverse asset and token support
3. Privacy
4. Superior, simple user experience

Given ZenGo's primary mission, it was imperative that security remained the top priority, and they focused on solving two long-standing challenges: problematic private keys and difficult - or *impossible* - account recovery.

We are well aware that replacing a recovery phrase with a password will not ultimately solve the problem of lost or stolen keys, as either can leave funds locked in wallets and abandoned forever. A business-critical issue, not solving this important matter could easily prevent mass adoption of crypto assets.

ZenGo's keyless security model removes the single point of failure of traditional cryptocurrency management solutions and frees the user from concern about their private keys being lost or stolen. Their unique approach replaces traditional private keys with two independently created "mathematical secret shares." One share is stored on a personal smart device or webcam-enabled system, the other on the ZenGo server.

Using a distributed key generation protocol (based on open source multi-party computation) to generate each secret key separately, no party has access to the other's secret. They also created a distributed signing protocol so both shares are always required to sign transactions on the blockchain. The user's shares never leave the device that created them, and with no single point of failure, even if something happens to one of the shares, the assets remain safe.

"

We encourage you to test the system for yourself by trying to restore your account with a picture or video of your face. It will fail, and you can rest assured those pictures of you on Facebook won't unlock your ZenGo account.

"

-- Tal Be'ery, Co-founder and Security Research Manager, KZen

If users lose a device, delete an app, or want ZenGo on a new device, they can recover their account with a simple face scan to match the 3D FaceMap created during the initial backup process. This allows the encrypted device share to be decrypted on the new device and the wallet quickly restored. With a simple, intuitive, fast interface, the ZenGo wallet is easier to use than any other option.

The Business Problem

According to research firm Statista, by the end of 2019, there were over 44 million crypto wallet users, a five-fold increase over a three-year period. It is expected when cryptocurrencies become more stable and the security questions are substantially answered, the rate of wallet use will skyrocket. Several factors for usage include a rise in crypto currency offerings and value; addressing security concerns from unintended use, device damage and theft; heightened user expectations; and continued global increases in general mobile use. But without robust access security, the advancement of the crypto industry would suffer. To mitigate security concerns in KZen's use case, effective authentication safeguards will ensure that only legitimate users are allowed access.

In addition, to create a commercially viable product, costs to KZen, and the user and business experiences must clearly benefit from authentication solutions, providing clear, positive impact on a company's image and bottom line.

Authenticating a user – verifying they are legitimate, and alive and physically present at the time of the login request – is a key requirement. However, unless the specific problem of recovering lost access through misplaced or stolen keys was fully resolved, all other issues and benefits would be of no consequence, and wallet acceptance could easily flounder.

KZen recently released the Android version of ZenGo, their highly anticipated crypto currency wallet with 3D Face Authentication and account recovery powered by FaceTec.

Choosing the Authenticator

To safeguard the highly sensitive, valuable assets cryptocurrency wallets manage, a truly secure access method must meet the following criteria:

- Ensure the user requesting access is verified as authorized *and* - to prevent spoofing – verify they are alive and present *at the time of account login*
- Be fast, 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, and recognizing the value of the iBeta certifications and a history of millions of users on six continents, the Facetec's 3D Face Authentication solution met or exceeded KZen's demanding usability and security requirements when tested in a wide variety of common environmental and situational circumstances with a diverse user base.

KZen considered and tested numerous purported face authenticators from several vendors, many claiming capable liveness detection, including a solution that flashed random colors at the user's face. By after testing, the choice was clear.

> *"We encourage you to test the system for yourself by trying to restore your account with a picture or video of your face," said ZenGo Co-founder and Security Research Manager, Tal Be'ery. "It will fail, and you can rest assured those pictures of you on Facebook won't unlock your ZenGo account."*

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. Available for all smart devices and webcam-enabled systems, FaceTec leverages decades of computer vision and artificial intelligence experience to ensure positive identification verification, three-dimensionality and human liveness.

Having funds secured by a face scan can be unnerving, especially knowing that technologies like Apple's Face ID have been defeated before. But as ZenGo CEO Ouriel Ohayon says, they use FaceTec authentication because it's been "battle tested over millions of users including banks", and it "cannot" be gamed.

Assessing 2D Facial Recognition: Two-dimensional facial recognition can be very effective at matching the face a device's camera sees to a stored photo taken at a similar angle and lighting conditions, and it is necessary in making a positive ID. However, 2D face matching cannot provide enough image data (signal) to distinguish between a photo or video spoof and a live person. Without robust Liveness Detection and 3D depth detection, it is not possible to anchor a human identity to an account for digital verification. Some 2D face matchers require users to blink, wink or nod randomly, but are easily fooled by simple spoof attempts like, "Photoshopping" eyelids on a copy of a photo and toggling between the two. Further, 2D photos can even be made to smile, talk, nod and look around using simple deepfake programs like CrazyTalk.

FaceTec 3D Face Authentication is trusted to stop fraud and identity theft by organizations of all sizes on six continents in banking, government, IAM, connected transportation and more.

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

The two primary 3D face authentication approaches are either hardware- or software-based. Hardware-based 3D 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: a 3D object is not necessarily a real person. Dolls, masks, 3D prints and wax figures are all 3D, but not alive. Every 3D face verification hardware solution released can be fooled by at least one of these artifacts.

FaceTec's software measures perspective distortion to prove the user's face is 3D and measures several dozen uniquely human traits. It converts a two-second video selfie into a proprietary biometric 3D FaceMap that contains the data to make an exceptionally accurate face-matching decision *and* a highly trusted liveness decision. AI-driven continuous learning makes authentication more effective over time, and FaceTec continually updates algorithms to guard against new threats. The FaceMaps are encrypted and securely stored in the cloud, the liveness data – half the required login data – is deleted immediately, preventing theft and fraud, and allowing users to securely authenticate across operating systems and multiple devices, ideal for large scale deployments.

For more information about FaceTec 3D Face Authentication can solve your most challenging authentication problems, please visit FaceTec.com.

The ZenGo Biometric Account Recovery Solution

In an industry-first, biometric-based ZenGo Account Recovery can now re-establish the digital identities of their users through the simple act of taking a selfie. Advanced 3D FaceMap technology quickly and securely authenticates users and unlocks their digital identities to allow them to easily regain access to their accounts after the loss or theft of their devices.

In addition to providing this critical service and a superior 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. Given the complexity and the importance of verifying identities digitally in real-time, FaceTec's authentication solution ensured the correct user is present and alive.

For a primer on the critical importance of Liveness Detection, please visit Liveness.com

Put Your Bitcoin Where Your Mouth Is!

ZenGo showed the skeptics that their system was secure enough to protect users crypto wallets by issuing a challenge on their blog:

"We're all about putting our money where our mouth is. We've designed ZenGo to be super convenient and super secure against attacks or errors of all forms and we have completed two security audits to prove it (1 and 2). Since we launched, we've received many questions about our innovative security model. "Where's the private key?" and "What happens if someone gets my email or a photo of my face?" are just a few of the questions we've received. We've written lots about these questions in our blog posts.

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

"Since we feel pretty confident in ZenGo's security, we figured we'd show you just how secure it is. And to prove it we've put 1 BTC in a wallet just waiting for you. All you need to do is break into the wallet and take it. If you can, the bitcoin is yours. Bitcoin just broke $11,000 so get to work ☺."

FaceTec's 3D Face Authentication exceeded the security and usability requirements for KZen's use case, ensuring the account recovery experience provided real users a superior user experience, and allowing them to very quickly and simply regain control over their high value crypto accounts.

FaceTec's 3D Face Authentication:

- Is iBeta Level 1 & Level 2 certified against presentation attacks
- Matched 3D face images with extreme accuracy
- 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)
- Enrolled users consistently and reliably
- Enrollment took only 10-15 total seconds

For business inquiries, please visit: https://dev.zoomlogin.com/zoomsdk/#/quote.

Further leveraging FaceTec's advanced technology, KZen recently announced a proof-of-concept of the first Threshold Signatures wallet for Facebook's proposed disruptive Libra blockchain digital currency testnet. Libra, with this technology, has the potential to reshape the financial landscape.

FaceTec, itself, had upped the ante when it introduced the world's first spoof bounty program in October of 2019. The goal of the $75,000 global, ongoing bounty program is to uncover potentially unknown vulnerabilities in the Liveness AI and security layers so any issues can be patched and the anti-spoofing capabilities and overall platform security elevated even further. To date, more than 13,000 spoof attempts by experts from around the world have been unsuccessful.

Recommendations

When deciding on a biometric authenticator, several factors must be considered. Security, usability, cost and future flexibility must be evaluated together.

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

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

To learn more about ZenGo and KZen Networks, please visit zengo.com.

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 in real-time at login. Other face biometrics tested met one or two of the required authentication attributes. FaceTec's solution managed all 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, and *must also* offer an open spoof bounty program to provide the very highest level of real-world vulnerability testing.

To learn more about Zengo's security, watch this video.

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. FaceTec's fast, simple selfie interface proved easy to use, even for the least tech savvy.

Usability must also be considered for IT management. FaceTec's 3D Face Authentication can perform user authentication without IT intervention: a liveness determination allows or blocks account access and sends a pass-fail decision to the customer application. No additional processing is required, except when an organization requires additional steps, such as document verification.

3. *Total Cost*: Overall costs must consider all direct and indirect expenses, as well as any projected savings from reductions in support overhead, breach mitigations and damage to hard-won branding.

Use licenses, subscriptions, in-house development or outright purchase costs are just the beginning of a realistic cost assessment. Support requirements must also include server setup and maintenance, additional hardware and

personnel, coding and interface customization, 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 potentially very expensive brand damage.

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

For press inquiries and additional information about FaceTec and Liveness.com, please contact John Wojewidka, VP of Communications, at johnw@facetec.com.

Summary

By anchoring a user's human identity to their digital identity through robust liveness detection, ZenGo users can - for the first time ever - now securely access their accounts even after losing or damaging their devices without remembering their keys, PINs or passwords. In this demanding environment, where fraud is a troubling constant, yet users cannot be inconvenienced, FaceTec was considered the perfect security solution for ZenGo. Every aspect of FaceTec's 3D Face Authentication, from security to usability to costs, validated the solution as the best cross-platform biometric access method, exceeding KZen's user's expectations and requirements.

- *Security*: Seamlessly, 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 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

Additional Resources

White Papers

- FaceTec – 3D Matching: 1/4.2M FAR@<1%
- Liveness, Biometrics' Final Frontier?
- PAD Testing, There's a New Sheriff in Town
- Anchoring Identity, From KYC to Finish
- FaceTec – 3D Liveness Methodology
- FaceTec – Internal Testing Guidance

Case Studies

- FaceTec – Jumio: Partner Case Study
- FaceTec – Turbi Car Sharing Case Study
- FaceTec – IAV Connected-Car Case Study

ZoOm Documentation

- FaceTec – Authentication Configurations
- FaceTec – Server & Cloud Architecture
- FaceTec – Frequently Asked Questions
- FaceTec – Frequently Asked Questions
- FaceTec – Passport Morphing Prevention

Latest FaceTec News

- FaceTec in the Media

FaceTec Spoof Bounty Program

- FaceTec $75,000 Spoof Bounty