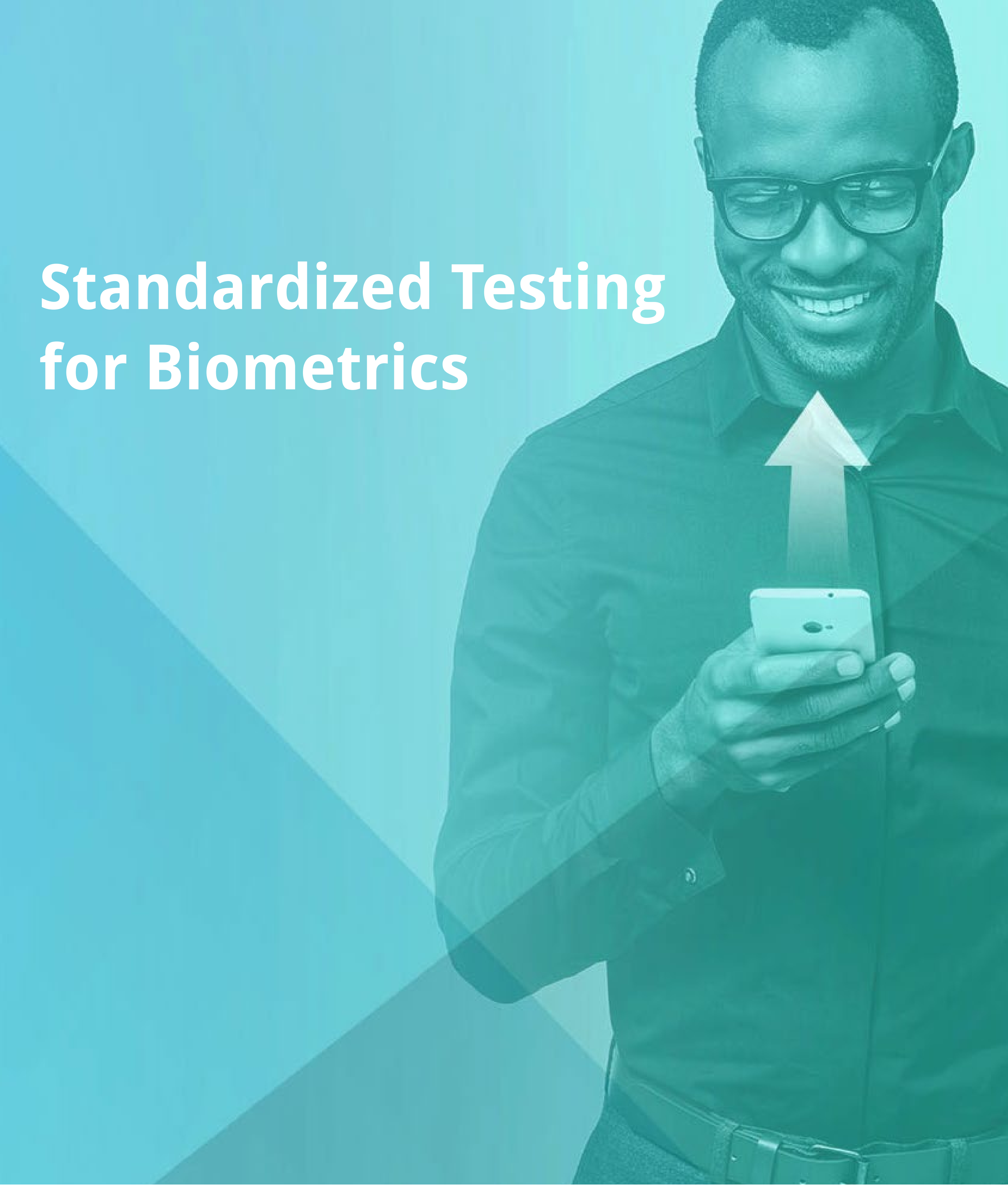
Standardized Testing for Biometrics



CUTTING THROUGH THE HYPE AND
FINDING INTEGRITY IN DIGITAL IDENTITY

facetec

There's a New Sheriff in Town

STANDARDIZED ANTI-SPOOF TESTING BRINGS LAW AND ORDER TO THE 'WILD WEST'

Standardized biometric presentation attack detection (PAD) testing is finally here, bringing accountability to the Biometrics industry, itself charged with providing trust in cyberspace. Over the past five years, the biometrics industry has experienced massive growth thanks to the integration of biometric hardware in consumer smartphones. The mainstream popularity heavily promoted by the likes of Apple, Samsung and Google helped biometrics overcome the privacy stigma derived from its use in law enforcement and created a paradigm shift allowing biometrics to become a must-have for a premium user experience.

The catalyst for more convenient device access, Biometrics have also since become a standard hardware feature on many lower-tier smart devices. But uninformed enthusiasm along with massive sensor fragmentation created a technological frontier often likened to the Wild West by industry analysts. With virtually no structured PAD testing available, biometric security testing was narrowly focused on algorithm vs. algorithm performance, not real-world applications, leaving the industry on the honor system when reporting anti-spoofing capabilities. "Optimistic" in-house, self-attested results led to overly-hyped marketing claims making it impossible for customers to understand and assess security performance.

Thankfully, third-party standardized testing is here to elucidate PAD performance, fact-check the claims being made, and ensure this industry selling trust can actually be trusted.

PART ONE

Biometrics are Everywhere

THE PROMISE AND PROLIFERATION OF BIOMETRICS

Biometrics ship as a standard feature on many smartphones and are quickly becoming integrated into more onboarding processes and mobile apps for easier logins. The value proposition is based on a balance of convenience and security, minimizing user friction in transactions traditionally made tedious in response to higher risk.

On the most relevant level, the use case of biometrics as a password replacement best illustrates the benefits of user authentication. Everyone knows passwords are all-too easy to share, phish and forget. That’s why even the most recent IT security reports still show the most used passwords are absurdly simple, like “12345678”, “password”, “football”, etc.[1]

The theory behind using biometrics in lieu of passwords is that biometric authentication removes the friction of having to invent, remember and change complex passwords regularly. And if your access credential is something you are, it will never be forgotten. Any biometric data unique to you should allow you alone to securely access your account.

And that is just the simplest example. Biometrics are beginning to be used in a wide range of vertical markets. In finance, healthcare, government, elections, retail, enterprise, connected living and more, biometrics promise to make life easier and more secure.

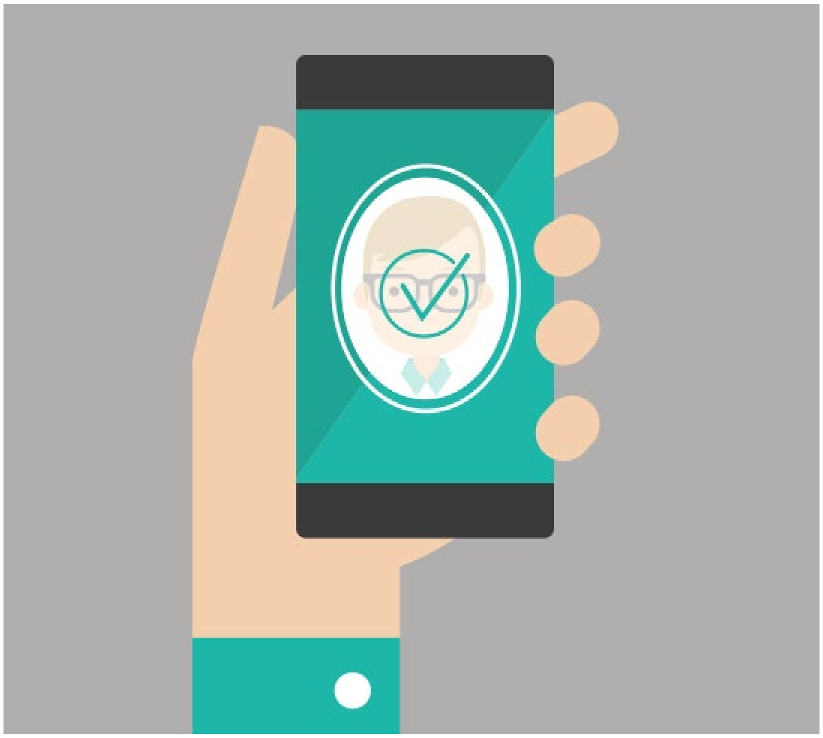
Use cases for biometrics across these markets include:

- Unlocking a phone
- Password replacement for mobile app
- 2FA, MFA & Strong Customer Authentication for PSD2
- Remote onboarding and proof-of-life for online account creation
- Time and attendance workforce management
- Age verification for the sale of controlled substances
- Authentication for payments and other financial transactions
- Voter registration in democratic elections

- Access management of electronic health records
- Unlocking a door lock or car door with a smartphone

The mobile biometrics market is skyrocketing, with industry leading research from Acuity Market Intelligence indicating revenues for the sector, which hit $6.5 billion in 2017, are on track to reach $50.6 billion by 2022.[2] Another report from Market Research Future, focusing solely on face recognition, forecasts a value of $8 billion by 2022[3] for that modality alone.

Biometrics, specifically face recognition and other device-agnostic, software-based solutions, are becoming the access control technology of choice. But what if they are not as good as they claim? What if we, as users, have not even been asking the right questions?



[1] http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/

[2] https://findbiometrics.com/mobile-biometrics-market-50-6-billion-acuity-409141

[3] https://findbiometrics.com/facial-recognition-market-8b-2022-report-508171

PART TWO

The Problem

A LACK OF STANDARDS PROMOTES HYPE AND VULNERABILITY

Above, we used the simple use case of password replacement to illustrate the value proposition of biometrics. While they promise convenience and security, it is the former that has driven decentralized adoption. Device access happens dozens of times a day and, from a user experience standpoint, reducing security levels just makes sense. However, that same lenient security has prevented centralized adoption.

Conventional wisdom says that your biometric data is yours and yours alone, so only you should be able to use it. But when a biometric is used to protect something of value, hackers will attempt to fool the system with presentation attack artifacts (non-human representations of the real thing), otherwise known as “spoofs”. The best biometric authenticators are built to thwart such spoofing attempts, in which a derivative of the users biometric data, like a face photo or video, is presented to the camera to try to trick the algorithms into accepting a facsimile.

It seems an obvious security requirement that a user be physically present in order to gain access, but biometric authentication is only as strong its ability to concurrently match unique human characteristics and verify living human traits in real-time. As it stands, truly verifying human liveness is hard. Really hard. This decades-long need for a “Turing Test in reverse” has spawned such non-biometric attempts as CAPTCHA, reCAPTCHA and “I am not a Robot”, steps in the right direction, **but still fallible.**

Even highly publicized biometric systems, like Apple’s Face ID, which leverages a 3D infrared camera system and claims to be the most secure biometric security in the consumer mobile market, was subject to a public spoofing by, among many others, security firm Bkav, that **bypassed** the 3D feature fairly easily using a mask with a paper face glued to it. This scenario proves to be particularly illustrative of the need for standardized third-party testing. Bkav did not publish detailed methodology for its Face ID spoofing process (though others published their own), and Apple never formally responded to the attack with a fix. In a self-attested security market a consumer be only become confused. While this was the highest profile example, dozens of solutions on the market continue to make unsubstantiated claims of immunity against presentation attacks.

Biometric hubris is not the solution to our password problems.

A data breach will tarnish a company's reputation, generate lawsuits, and now, thanks to Europe's General Data Protection Regulation (GDPR), result in **massive fines**. Not surprisingly, the number-one cause of data breaches is compromised password credentials. High-definition images of faces, irises and fingerprints can be captured by bad actors at a distance, but that's not even necessary for many social media users who already choose to post this biometric data themselves. So despite biometric vendors' eagerness to promote solutions without fully-developed liveness detection, replacing passwords with algorithms that will accept artifacts created from commonly available sources as the genuine articles will simply not work.

Thankfully, trust is on the way.

PART THREE

Putting Trust To The Test

WHAT KEEPS THE BIOMETRICS SECURITY CLAIMS HONEST?

Beyond in-house testing, third-party biometrics testing programs now exist that vendors can utilize to publically validate their solutions.

Government and Industry-specific Regulations

Certain high risk sectors already have broad IT provisions concerning the protection of data and accountability. Historically, such provisions have shed light on the inflated marketing hype in the biometrics industry. HIPAA, the Health Insurance Portability and Accountability Act, for instance, is a generalized security standard in the healthcare market which has long been thought of as a space ripe for biometric adoption. The presence of this and other healthcare security standards, however, are often cited as reasons why biometric adoption has been slow in clinics and hospitals.

Similarly, government regulations like Europe’s Revised Payment Services Directive (PSD2) and the aforementioned GDPR mandate stronger-than-password authentication solutions with specific capabilities that enable control over user data and have strict penalties for non-compliance. Directives such as these are tangential to biometrics testing, but do attempt to set a high-water mark for security performance. However, the directives are too often written by non-biometrics experts and use language not specific enough to ensure the end goals are met.

Let’s take PSD2, for example. The directive reads:

“Strong customer authentication means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent.”

But the directive means:

Strong Customer Authentication dictates that certain industries require their customers to provide at least two of the three following factors:

1. A mutually shared secret, like a password or security question answer
2. A personal device unique to them, like a hardware token or mobile phone
3. A face scan, voice recording or fingerprint photo matched to a server-side counterpart

While the original language leaves much detail to be desired, the spirit is clear and correct. It is time for industry best practices to be pushed far beyond the abilities of even highly sophisticated cyber criminals and these rules will drive rapid technology advancements, particularly in AI.

Bounties

Collaboration is ingrained in the IT community, and bounties have long been a method of battle-testing the integrity of security systems with the goal of making them more robust. Open bounties for finding security vulnerabilities encourage researchers and hackers to report flaws in security systems to the vendor rather than exploit them.

Bounties have proven indispensable to large firms like Google and Microsoft that deal with vast amounts of valuable user data, but must be properly incentivised to work. As security becomes more sophisticated thanks to the introduction of biometrics and multiple factors, or modalities, vendors must ensure they are not essentially outbid by interested parties looking to buy zero-day vulnerabilities on the black market.

Unfortunately, since most biometrics security providers know their systems cannot even stand up to rigorous *in-house* testing, they have rarely offered external bounties, preferring plausible deniability while hoping their vulnerabilities aren't highlighted on YouTube or exposed on nefarious dark-web sites.

NIST

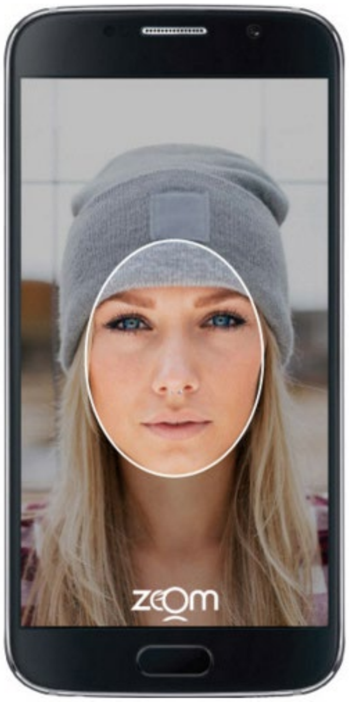
The most visible standardized biometric testing has been conducted by NIST (the National Institute of Standards and Technology). Their algorithm evaluations include fingerprint, face recognition, iris and tattoo biometrics, in addition to multi-biometric solutions carried out in 2007 and 2009 during the technology's nascency.

The NIST evaluations are conducted in accordance with set challenges and the organization's schedule. Ongoing evaluations for fingerprint (MINEX) and iris (IREX) have long been touted by top performers as badges of excellence, particularly in the realms of law enforcement and border security. They test homogenized biometric modalities used by the law enforcement and surveillance industries using narrow testing criteria that does not include Presentation Attack Detection.

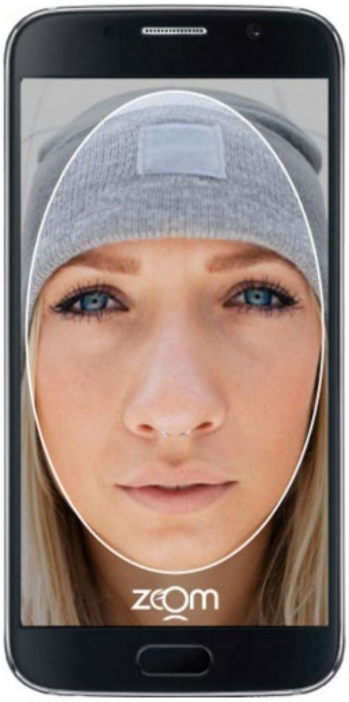
Unfortunately, since matching performance has been sole the focus of the NIST testing, it has created millions of armchair biometrics experts who love to ask "What's the FAR?" (False Accept Rate) of every new algorithm they see, while having little understanding of several important factors, including FRR (False Recognition Rate) and training vs. test sets. Most importantly, they have essentially zero understanding of the liveness detection required for real-world authentication. This lack of liveness detection testing by NIST left the the biometrics industry focused on FAR and resulted in little attention paid to anti-spoofing until just a few years ago. It is encouraging to see the industry, and NIST certified labs, finally beginning to understand the critical importance of anti-spoofing, and new testing standards being created to provide insight into biometric authenticator security levels.

iBeta

Based in Denver, Colorado, iBeta performs independent third-party testing and certification for all biometric modalities, and has created the world's first certified Presentation Attack Detection (PAD) test based on the recently released ISO 30107-3 standard. Accredited by NVLAP (National Voluntary Laboratory Accreditation Program), iBeta is the only NIST-certified biometrics testing lab. iBeta's equipment, experience and methodology are invaluable when determining the PAD security level of a biometric, and their test results carry significantly more weight than any in-house or private testing.



ZoOm observes the user's head, neck, ears, hair, facial features and their environment as the camera is moved closer to the face. During the motion, the camera's view of the face changes and perspective distortion will be observed if the face is 3D.



Conversely, no distortion occurs with 2D objects like photos or videos. FaceTec's proprietary algorithms capture ~30 video frames while tracking the motion of the device. The result is a dynamic perspective, 3D face authentication from a standard 2D camera.

iBeta's biometric testing programs are wide-ranging.
The lab is equipped to test for:

- CBEFF, BioAPI, and data interchange
- Interoperability
- Performance testing (FAR, FRR, FMR, FNMR)
- Spoofing and liveness testing
- Presentation attack detection
- Scenario testing
- Coordination Mil-Std 810 G
- DEA EPCS biometric subsystem certification

Important note: The ISO 30107-3 standard requires test subjects be "Fully Cooperative Users" and provide "any and all" biometric data requested by the testers. This makes the iBeta PAD test significantly harder than tests using only publicly available biometric data or non-cooperative subjects. The goal is to ensure the authenticator's liveness detection is strong enough to combat complicit user fraud, synthetic ID fraud and phishing attacks.

FIDO Alliance

In 2018, the FIDO Alliance introduced its own Biometric Component Certification Program. The intention is to address the historical lack of standards with unbiased accredited laboratory testing. A global benchmark indicating a biometric solution is fit for commercial use, FIDO's Biometric Component Certification Program – based on the NIST-certified iBeta testing procedure – adheres to ISO standards (ISO/IEC 19795; ISO/IEC 30107), and tests for Presentation Attack Detection.

Important note: Though the testing criteria is not yet finalized, currently it does not appear that the FIDO PAD test will require the testers to be "Fully Cooperative Users" as the ISO standard requires. This means it is possible the test results may not be as definitive in its determination as to whether or not the authenticator is robust enough to prevent complicit user fraud and phishing attacks.

PART FOUR

The iBeta PAD Test

TESTING BIOMETRICS ACROSS THE BOARD, WITHOUT BIAS

“Our NVLAP-accredited lab and ISO-guided program provides the level of verifiability and consistency needed to help providers create products that can be more easily assessed and targeted for specific use cases,” said Dr. Kevin Wilson, Director of Biometrics at iBeta.

iBeta testing can be conducted on a production version of an authenticator, but it is recommended that it be conducted on a modified version. The modifications should include the ability to perform liveness on enrollment (the very foundation of the “trust chain”), and to allow thousands of attempts, with “lock-out”, and have “anti-reverse-engineering” mechanisms removed. However, when a production version lockout would have been triggered, the app should inform testers of the consequences of the lockout (e.g., to retry in five minutes or one hour). This helps testers better understand how many attempts they would have in the real world, and how long they would have to wait for additional attempts or if they would have to re-download the app.

> **“The iBeta test makes it much easier to differentiate between marketing hype and objectively-verified security. To us, there is no doubt that formalized, standards-backed PAD tests like iBeta’s should be a prerequisite for every biometric vendor.”**
>
> - Kevin Alan Tussy, CEO, FaceTec

Testing is typically conducted over two-to-three weeks on two contemporary smart devices, and in accordance with the level of spoofing and techniques needed to create artifacts of the genuine biometric for use in the presentation attack. The test subjects used in the test effort are “fully cooperative, ” meaning they willingly provide any and all biometric samples, including high quality photos and videos of their likenesses. If the test includes liveness on enrollment, then only non-living artifacts are used to try to fool the system into enrolling an inanimate object in place of a living person. The test time for each subject is approximately eight hours. At least 5-6 species of presentation attacks (PAs) are expected and will be attempted five times each for each subject, for a total of approximately 1500 presentation attack attempts.

WATCH: In this video we show you how to create a realistic 3D animated spoof from a 2D photograph using CrazyTalk software.

At the conclusion of the PAD testing, the real, living test subject returns and authenticates three times successfully to verify that the authenticator application is still able to recognize the genuine subject, and hasn’t just been altered to rebuff all attempts.

PART FIVE

ZoOm®, PAD Certified to Level 1

PAD CERTIFICATION IS DIFFICULT, BUT PROVEN TO BE ACHIEVABLE

ZoOm 3D Face Login from FaceTec was the first biometric authenticator in history to achieve 100-percent anti-spoofing results in the iBeta Level 1 Presentation Attack Detection (PAD) Certification test.

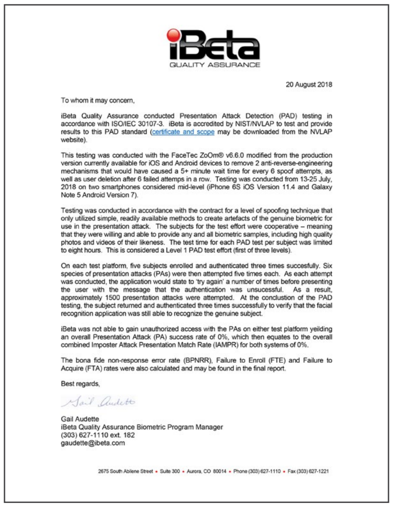
Powered by Artificial Intelligence, ZoOm creates a 3D image of a user's face using a standard 2D camera. Because it is biometric software, ZoOm is device-agnostic and can be used on any smart mobile device with a selfie camera, or webcam-enabled system using a modern browser. Demo apps are currently available for download on iOS, Android and webcam-based systems.

The milestone PAD certification result was achieved by subjecting ZoOm 3D Face Login to more than 1,500 spoofing sessions over a period of six days, between July 13–25, 2018. Not one attempt succeeded in fooling FaceTec's technology. iBeta tested ZoOm against complicit user fraud and phishing-style attacks as required by the ISO standard 30107-3, in which the cooperative test subjects aided in the presentation attacks.

Once the spoofing onslaught concluded, the enrolled user then successfully authenticated on the tested device three times. This confirmed that ZoOm's security scheme had not been altered to reject all attempts and could still differentiate between the correct user and a spoof, even after hundreds of rigorous attempts.

The version of ZoOm tested by iBeta was modified to remove lockout features but the underlying technology was exactly the same as the demos available for download. Anyone with an Android or iOS smartphone, or webcam can now employ third-party Certified Level 1 biometric security.

In attaining a perfect score, FaceTec proved that commercially available and affordable face authentication software can stand up to the highest levels of third-party testing scrutiny. While some may argue the benchmark is too high to be viable, biometrics vendors must be pushed to develop measurably robust technology that can rebuff the bad actors in today's increasingly dangerous cyber-landscape. No one should have to settle for biometrics solutions that haven't passed tests proving that they are capable against a wide range of presentation attacks.



iBeta
QUALITY ASSURANCE

20 August 2018

To whom it may concern,

iBeta Quality Assurance conducted Presentation Attack Detection (PAD) testing in accordance with ISO/IEC 30107-3. iBeta is accredited by NIST/NVLAP to test and provide results to this PAD standard (certificate and scope may be downloaded from the NVLAP website).

This testing was conducted with the FaceTec ZoOm® v6.6.0 modified from the production version currently available for iOS and Android devices to remove 2 anti-reverse-engineering mechanisms that would have caused a 5+ minute wait time for every 6 spoof attempts, as well as user deletion after 6 failed attemps in a row. Testing was conducted from 13-25 July, 2018 on two smartphones considered mid-level (iPhone 6S iOS Version 11.4 and Galaxy Note 5 Android Version 7).

Testing was conducted in accordance with the contract for a level of spoofing technique that only utilized simple, readily available methods to create artefacts of the genuine biometric for use in the presentation attack. The subjects for the test effort were cooperative – meaning that they were willing and able to provide any and all biometric samples, including high quality photos and videos of their likeness. The test time for each PAD test per subject was limited to eight hours. This is considered a Level 1 PAD test effort (first of three levels).

On each test platform, five subjects enrolled and authenticated three times succesfully. Six species of presentation attacks (PAs) were then attempted five times each. As each attempt was conducted, the application would state to 'try again' a number of times before presenting the user with the message that the authentication was unsucessful. As a result, approximately 1500 presentation attacks were attempted. At the conclustion of the PAD testing, the subject returned and authenticated three times successfully to verify that the facial recognition application was still able to recognize the genuine subject.

iBeta was not able to gain unauthorized access with the PAs on either test platform yeilding an overall Presentation Attack (PA) success rate of 0%, which then equates to the overall combined Imposter Attack Presentation Match Rate (IAMPR) for both systems of 0%.

The bona fide non-response error rate (BPNRR), Failure to Enroll (FTE) and Failure to Acquire (FTA) rates were also calculated and may be found in the final report.

Best regards,

Gail Audette

Gail Audette
iBeta Quality Assurance Biometric Program Manager
(303) 627-1110 ext. 182
gaudette@ibeta.com

2675 South Abilene Street • Suite 300 • Aurora, CO 80014 • Phone (303) 627-1110 • Fax (303) 627-1221

READ: iBeta ZoOm 3D Face Login SDK PAD Certification Test Report Executive Summary

A Solid Foundation For Innovation

NOW THE REAL WORK CAN BEGIN

Now the real work can begin

Standardized biometric PAD testing will prove to be a lynchpin for the industry, creating a solid foundation for building strong biometric authentication technology. Relying parties, from banks to hospitals to governments to everyday users, will be better informed when choosing biometrics that are objectively certified as secure enough for their intended use case. With a level playing field on which to assess the numerous solutions on the market, the biometrics vendors will be pushed to reach new heights of security, while providing fast and frictionless user interfaces. And while the standards may be rigorous and the competition fierce, no matter who captures the market share, the real winners will be the customers and their users. Though we opened with the familiar cliche, “There is a New Sheriff in Town,” is it more accurate to say, “There is *finally* a Sheriff in Town.”

About FaceTec

FaceTec provides class-leading biometric authentication solutions for mobile and web applications requiring certified, high-performance liveness detection. Leveraging decades of computer vision, artificial intelligence and advanced biometrics experience, FaceTec developed ZoOm, the iBeta PAD Level 1 Certified 3D face authentication platform for iOS, Android, mobile and desktop browsers/webcams. The only unphishable and unshareable biometric modality, ZoOm is ideal for onboarding and virtually any identity and access management requirement.

Founded in 2013 with offices in San Diego, CA; London, UK; and Summerlin, NV, FaceTec provides biometric security on five continents for organizations in financial services, mobile payments, border security, connected transportation and more. For more information and business inquiries, please visit www.ZoOmLogin.com.