EXHIBIT A

https://web.archive.org/web/20200927103934/https://www.ibeta.com/iso-30107-3-presentation-attack-detection-confirmation-letters/

INTERNET ARCHIVE WayBackMachine https://www.ibeta.com/iso-30107-3-presentation-attack-detection-confirmation-letters/ Go DEC SEP 27 JAN 2019 2020 2021 43 captures 17 Aug 2019 - 15 Oct 202 About this capture

Burger Navigation has no widgets. Please populate it. Appearance -> Widgets

info@iBeta.com
Call us: 303.627.1110
Follow:



ISO 30107-3 PRESENTATION ATTACK DETECTION CONFIRMATION LETTERS

In an effort to provide clarification and a better understanding regarding the ISO Presentation Attack Detection testing that iBeta conducts in accordance with the ISO/IEC 30107-3 standard and in alignment with the ISO/IEC 30107-1 framework, we provide the following explanation.

Confirmation Letters

iBeta posts, by written vendor consent, the Presentation Attack Detection (PAD) Confirmation letters that provide the results of the iBeta PAD testing. These letters specify the type of PAD testing and the configuration of the vendor product that was tested. In order to fully assess the vendor product, the audience of these letters should understand the test method used to assess conformance with the ISO 30107-3 Standard.

Understanding the Test Method

iBeta is accredited by NIST NVLAP as an Independent Test Lab and ISO 30107-3 is included in our scope of accreditation. As such, the specific test procedures, processes, and report templates, as developed by iBeta, are audited and approved as part of the NIST administration of the NVLAP.

Prior to test start, the PAD mechanism is determined:

- **PAD subsystem test – evaluates presentation attack detection only**
- **Data capture test – evaluates the coupled presentation attack and quality checks**
- **Full system test – evaluates the biometric comparison capabilities of the full biometric subsystem**

The type of PAD mechanism determines the ISO/IEC 30107-3 mandated reporting metrics for the evaluation. For subsystem PAD evaluations, the classification

error rates (APCER, BPCER and associated non-response rates) are determined whereas when evaluating full systems, the imposter attack presentation match rates (IAPMR and associated FNMR/FMR) is determined.

In order to specify more exactly the test method, iBeta identified levels of testing (although similar to the FIDO Alliance Levels A & B, there are significant differences). The testing levels and performance requirements are identified as:

Level	Time	Expertise	Artefact source	Limit
1	8 hours per subject or species	None	Cooperative subject and equipment is readily available in a normal home or office environment	0% penetration or match rate allowed
2	2-4 days per subject or species	Moderate – participated in at least 1 other PAD test with the target modality and has an understanding of the liveness detection functionality of the test target	Cooperative subject and equipment is more expensive (such as a 3D printer, resin mask, latex mask)	1% penetration or match rate allowed
3	Unlimited	Significant – has insider knowledge of the functionality of the test target and has participated in at least 2 other PAD tests with the target modality	Cooperative Subject and latent sources for subject data. Equipment is extensive e.g., special order contact lenses, facial silicone masks, and 3D printed spoofs	Not established

In order to maintain uniformity between vendor solutions and modalities and to apply the test methods to each vendor consistently, the 6 species of attacks (called "PAIS" in ISO 30107-3) are selected as uniformly as possible. If the application uses an active liveness detector to elicit a "voluntary response" (the ISO 30107-1 term), then the species of attacks are tailored just as an impostor would tailor them to provide the movement, smile, blink, etc. Our procedure sets a material cost limit such that Level 1 artefacts cannot exceed $30 and Level 2 are limited to $300. This keeps the artefacts creation or procurement costs generally consistent across all vendor solutions.

In addition, each species set of artefacts is created and applied to the PAD within a time limit. For Level 1, if liveness detection only is being assessed, then iBeta will create and apply each of the species artefacts within 8 hours, targeting to present 150 attacks alternated with 50 genuine presentations. If a full system is under evaluation, then the artefacts associated with the species for a single genuine subject are created and applied within 8 hours. With 6 subjects and/or 6 species, the testing therefore requires 48 hours.

ISO 30107-3 discusses cooperative versus uncooperative subjects. iBeta uses cooperative subjects in that the artefacts are created from biometric characteristics provided by volunteer data subjects (if not purchased) who are willing and able to pose for photos, record videos, provide their fingerprints in molding material or sit for a live cast. We only use cooperative subjects as the artefacts created from willing volunteers are of better quality making for a more conservative test. iBeta is evaluating the vendor solution and not the ability of our testers to obtain latent prints, as an example.

Prior to applying any presentation attack, the configuration of the vendor solution is recorded and the version is referenced in the confirmation letter. In addition, because the device used to capture the biometric sample impacts the results, the exact device configuration is recorded and also referenced in the confirmation letter.

During the test effort, bona fide biometric presentations to the PAD device not only provide the reporting metrics required by ISO 30107-3 but also provide the indication of usability by the data subjects. For this reason, iBeta is now limiting the BPCER and FNMR to 15% to obtain a "PASS" rating. If a bona fide data subject cannot be recognized as live and/or matching to the enrolment reference, iBeta will suspend testing as a high BPCER or FNMR biases the test result. These error rates were originally unconstrained but have been limited to 20% and now recently reduced to 15%. This limit is reviewed every 6 months and is subject to further reduction as PAD technology improves.

The iBeta testing and reporting provides results that indicate that the solution testing is compliant or conforms with the ISO 30107-3 testing and reporting requirements. This itself, however, does not translate to a certification of the vendor product.

Certification vs. Conformance

When iBeta was initially accredited, the term certification was used but was corrected during the NIST/NVLAP audit in March 2019. There is no difference in our test methods, procedures, or processes between the earlier testing and the testing after that date with the exception that the allowed limit for genuine or Bona Fide presentations is now stricter.

Confirmation Letters

Aware PAD Level 1 Confirmation Letter (PDF)

Aware PAD Level 2 Confirmation Letter (PDF)

FaceTec PAD Level 1 Confirmation Letter (PDF)

FaceTec PAD Level 2 Confirmation Letter (PDF)

HID Global M-Series PAD Level 1 Confirmation Letter (PDF)

HID Global M-Series PAD Level 2 Confirmation Letter (PDF)

HID Global V-Series PAD Level 1 Confirmation Letter (PDF)

ID R&D PAD Level 1 Confirmation Letter (PDF)

Idemia PAD Level 1 Confirmation Letter – Active Liveness (PDF)

Idemia PAD Level 2 Confirmation Letter – Active Liveness (PDF)

Idemia PAD Level 1 Confirmation Letter – Passive Liveness (PDF)

Idemia PAD Level 2 Confirmation Letter – Passive Liveness (PDF)

IDmission PAD Level 1 Confirmation Letter (PDF)

ImageWare PAD Level 1 Confirmation Letter (PDF)

Incode PAD Level 1 Confirmation Letter (PDF)

Innovatrics PAD Level 1 Confirmation Letter (PDF)

iProov PAD Level 1 Confirmation Letter (PDF)

iProov PAD Level 2 Confirmation Letter (PDF)

OCR Labs PAD Level 1 Confirmation Letter (PDF)

OCR Labs PAD Level 2 Confirmation Letter (PDF)

Redrock PAD Level 1 Confirmation Letter (PDF)

Thales Group PAD Level 1 Confirmation Letter (PDF)

Zoloz PAD Level 1 Confirmation Letter (PDF)

Zoloz PAD Level 2 Conformance Letter (PDF)

We offer a full range of on-demand QA software testing services. Our services encompass many different software quality activities such as: quality assurance, functionality testing, mobile testing, performance testing, browser and hardware compatibility testing, acceptance testing, and code reviews.

Our testing labs can handle just about anything.

Services

- Accessibility Testing
- Automated Testing
- Biometrics Testing
- Brand Auditing
- EPCS
- Game Testing
- Load / Performance Testing
- Localization Testing
- Mobile Testing
- Web Testing

Get in Touch

303.627.1110

2675 S Abilene Street

Suite 300

Aurora, CO 80014

For all job inquiries:

Drop Us A Resume!

https://web.archive.org/web/20230201190043/https://www.biometricupdate.com/202302/facetec-triples-scope-and-payout-in-spoof-bounty-to-thwart-biometric-liveness-attacks

INTERNET ARCHIVE Wayback Machine
https://www.biometricupdate.com/202302/facetec-triples-scope-and-payout-in-spoof-bounty-to-thwart-biometric-liveness-attacks
Go
JAN FEB 01 MAR
2022 2023 2024
15 captures
1 Feb 2023 - 23 Oct 2025
About this capture

Share
Tweet
Link
Comment

FaceTec triples scope and payout in Spoof Bounty to thwart biometric liveness attacks

Feb 1, 2023, 12:16 pm EST | Chris Burt

CATEGORIES Biometric R&D | Biometrics News | Liveness Detection



FaceTec has expanded its Spoof Bounty to both iOS and Android operating systems and tripled the total payouts available from $200,000 to $600,000 to help it identify potential vulnerabilities in biometric liveness detection.

Participants hunt for ways to defeat Facetec's 3D Liveness software in real-world conditions, demonstrating and improving upon its security in real-world conditions, not just in the lab, the company says. Rewards are paid out for any spoof or camera bypass attack that beats the system.

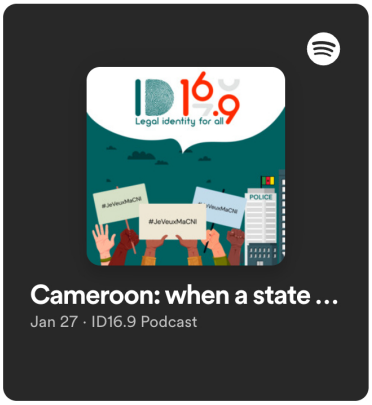
The company informed *Biometric Update* that about 10,000 people have participated in the program, including professors, competitors, government agencies and hackers. Two $30,000 bounties were paid about two and a half years ago for Level 1 attacks.

They revealed that certain kinds of screens could pose a problem when manipulated in a certain way, so FaceTec retrained its neural network models to catch this particular attack. The company has also learned from unsuccessful attempts, mostly about the popularity of different attack methods.

"We put our AI to the test so that users of the FaceTec software can be shown – and not just told – just how secure FaceTec's 3D Liveness Detection is," says Kevin Alan Tussy, FaceTec CEO. "We don't hide our product behind 'Request A Demo' forms. FaceTec stands behind its 3D Liveness software in a way that no 2D Liveness vendor will ever be able to replicate. After rebuffing more than 130,000 bounty program attacks over the last three years, we've learned a tremendous amount about potential threat vectors and how to stay ahead of them."

The Spoof Bounty program operates at five levels, the first three covering spoof artefacts of increasing complexity, and the last two addressing bypasses. Level 4 is for decrypting and editing the contents of the 3D 'FaceMap' with synthetic data, while Level 5 is for

THE ID16.9 PODCAST



All Podcast Episodes

MOST READ THIS WEEK

Face and fingerprint biometrics for retail payments advancing by inches
Fingerprint Cards anticipates bounce-back in smartphone biometrics revenues in 2023
8.6M fake ID users in UK: GBG report
Face biometrics mandated for SIM card activation in Argentina
Porn back as political hurdle for age verification in UK, Australia takes next step
Exponential hacking of biometric authentication reveals some defenses already overwhelmed
Is Kenya's 'big Huduma Namba thing' being adapted to digital-only ID or dropped for a UPI?
US border boost for biometrics suppliers as Customs, ICE contracts grow
How China outsells everyone on facial recognition surveillance
Welcome to high-class Manhattan, facial recognition. This will be interesting

successfully taking over the camera feed and injecting images, in each case leading to a Liveness Success response.

The program doubled in investment from $100,000 to $200,000 last year.

Article Topics

AI | biometric liveness detection | biometrics | bug bounty | FaceTec | research and development | spoof detection

Latest Biometrics News



Sierra Leone launches biometric ID card to upgrade CRVS, Kenya's UPI goes birth-to-death



EAB seminar plays down EU parliament's biometrics ethics concerns



Biometric liveness detection from OCR Labs shows no bias in BixeLab testing



Transparency can drive digital ID equity, policy forum panelists say



Digital ID financing quietly hums: Strata gets $26M from VCs, Saviynt gets $205M loan



Digital ID management software makers bought out by Veridos in Serbia, UST in Canada

Comments

Leave a Reply

Enter your comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Subscribe To The BiometricUpdate.com Email Newsletter

Stay on the cutting edge of the biometrics



Daily Biometrics News »

FEATURED COMPANY

facephi

Facephi, leading the revolution of digital identity verification

LEARN MORE

More Biometrics Companies »

BIOMETRICS RESEARCH

African demand for digital ID infrastructure growing, as is fraud: Smile Identity report

8.6M fake ID users in UK: GBG report

Digital ID experts to tackle fraud, deepfakes in high demand: OCR Labs report

More Biometrics Research »

BIOMETRICS WHITE PAPERS

Presentation attack detection: Measuring performance of APCER and BPCER

Tenprint fingerprint scanners: All you need to know

Multispectral imaging (MSI) fingerprint technology

More White Papers »

BIOMETRICS EVENTS

ID4Africa LiveCast – Civil registration in Africa: Scaling for impact
Online: Feb 8, 2023

Aviation Festival Asia 2023
Suntec, Singapore: Feb 28 - Mar 1, 2023

World Police Summit
United Arab Emirates: Mar 7 - Mar 9, 2023

More Biometrics Events »

EXPLAINING BIOMETRICS

3 ways to make biometrics work in the workplace

industry by subscribing to daily news updates from BiometricUpdate.com

LEARN MORE



- ID verification explainer: How does IDV tech work?
- Biometric speaker recognition expanding along with voice applications
- Explaining face biometrics applications and adoption
- CCTV networks and biometric surveillance
- More Biometrics Explainers »»

BIOMETRIC UPDATE.COM

Copyright © 2023 Biometrics Research Group, Inc. All Rights Reserved.

Web Design by Studio1337

https://web.archive.org/web/20260102202204/https://bixelab.com/confirmation-letter/

INTERNET ARCHIVE WayBackMachine https://bixelab.com/confirmation-letter/ Go OCT JAN 02 FEB 2024 2026 2027 About this capture
13 captures 27 Sep 2023 - 2 Jan 2026

Independent Testing & Accreditations

BixeLab is an independent biometric testing laboratory with NVLAP and FIDO accreditations, specializing in biometric performance evaluation, reporting, and testing for presentation attack detection, bias and injection attack testing. For a full list see here.

NVLAP TESTING NVLAP LAB CODE 600301-0 ilac-MRA

fido ALLIANCE

NVLAP Accreditation Details

FIDO Accreditation Details

CONFIRMATION LETTERS

BixeLab Letters of Confirmation for the testing undertaken on various biometric products are provided below. This table specifies the testing that was undertaken, details of the provider, product, and product version in addition to the relevant standards where applicable. The featured letters are published with the endorsement of supplier, technology, or solution providers. This list includes only standard evaluations such as biometric presentation attack detection (PAD) ISO/IEC 30107-3 and instances where providers have agreed to disclose their results

BixeLab takes pride in offering biometric testing services that are both trustworthy and reliable. Click on the PDF links for further details associated with the testing completed. Contact us or check our FAQ page for more information.

10 entries per page Search:

Date of Issue	Provider	Product tested	Product Version	Modality	Testing type	Tested to
2025-10-27	FaceTec, Inc.	FaceTec SDK	Mobile v9.7.83, Web v9.7.76	Face	Injection Attack Detection (IAD)	CEN/TS 18099
2025-10-27	FaceTec, Inc.	FaceTec SDK	Mobile v9.7.83, Web v9.7.76	Face	PAD Level 1	ISO/IEC 30107-3
2025-10-27	FaceTec, Inc.	FaceTec SDK	Mobile v9.7.83, Web v9.7.76	Face	PAD Level 2	ISO/IEC 30107-3
2025-10-27	FaceTec, Inc.	FaceTec SDK	Mobile v9.7.83, Web v9.7.76	Face	PAD Level 3	ISO/IEC 30107-3
2025-10-09	AwareID	AwareID	v3.3.008	Face	PAD Level 1	ISO/IEC 30107-3
2025-10-09	AwareID	AwareID	v3.3.008	Face	PAD Level 2	ISO/IEC 30107-3
2025-09-24	Xperix Inc.	RealScan SG10 and RealScan SG10i	v2.1.0.1951	Fingerprint	PAD Level 1	ISO/IEC 30107-3
2025-09-24	Xperix Inc.	RealScan SG10 and RealScan SG10i	v2.1.0.1951	Fingerprint	PAD Level 2	ISO/IEC 30107-3

2025-09-16	Cybertech JSC Vietnam	BKACS device's BKACS-FACE	v1.0	Face	PAD Level 1	ISO/IEC 30107-3
2025-09-16	Cybertech JSC Vietnam	BKACS device's BKACS-FACE	v1.0	Face	PAD Level 2	ISO/IEC 30107-3

Showing 1 to 10 of 46 entries

Expression of Interest for BixeLab Services

BixeLab

Standards-based testing and certification of biometrics, digital identity and AI solutions to assure accuracy, security and fairness.

Level 1, Endeavour House, 1 Franklin Street, Griffith, ACT, 2603, Australia

ABN 86 648 170 263

Privacy Policy

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept", you consent to the use of ALL the cookies.

Cookie settings ACCEPT

https://web.archive.org/web/20250209015020/https://idtechwire.com/3d-vs-2d-biometrics-part-2-jay-meier-on-liveness-detection-and-revolutionizing-idv/

INTERNET ARCHIVE Wayback Machine
https://idtechwire.com/3d-vs-2d-biometrics-part-2-jay-meier-on-liveness-detection-and-revolutionizing-idv/
Go
1 capture
9 Feb 2025
JAN 2024 FEB 09 2025 MAR 2026
About this capture

3D vs. 2D Biometrics, Part 2: Jay Meier on Liveness Detection and Revolutionizing IDV

January 14, 2025

Following Part 1 of our deep dive into 3D biometrics with FaceTec VP Jay Meier, the conversation delves even deeper into the innovations driving FaceTec's technology—and its new UR code protocol.



Jay highlights the transformative power of 3D systems over 2D systems, explaining how FaceTec's approach captures over 100 video frames during authentication to create unparalleled depth of data. This process, he notes, doesn't just provide better matching accuracy; it redefines what is possible in terms of liveness detection and fraud prevention.

"By measuring the changes in perspective distortions as the camera moves, we're effectively creating a new biometric," Jay explains. "It's not about simply detecting a face—it's about understanding the unique curvature and three-dimensionality of that face."

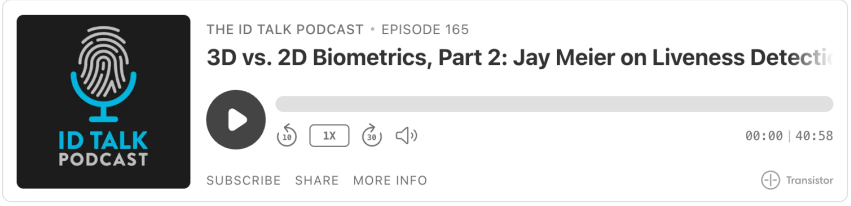
The discussion also explores how FaceTec's system mitigates risks like presentation attacks and deepfake injection. By leveraging 70+ involuntary human cues and encrypting biometric data at every stage, FaceTec ensures that its system is resilient against even the most sophisticated attacks.

"Cryptography is essential," Jay says. "We encrypt data six ways from Sunday and alter files after use so that stolen data is completely unusable."

Jay also outlines the groundbreaking UR Code protocol, which combines efficiency, privacy, and interoperability to solve some of the industry's most pressing issues. Unlike other solutions, FaceTec's UR Code doesn't require live pings to government databases, instead enabling secure verification through a lightweight, digitally signed 2D barcode.

"It's a protocol, not a product," Jay emphasizes. "We think it's going to revolutionize identity management on the internet. The fire is lit."

Listen to Part 2 of this fascinating discussion wherever you get your podcasts, or through the media player below:



–

January 14, 2025 – by the ID Tech Editorial Team

Related News



PARTNERS

facetec

FaceTec's patented, industry-leading 3D Face Verification and Reverification software anchors digital identity, creating a chain of trust from user onboarding to ongoing authentication on all modern smart devices and webcams. FaceTec's 3D FaceMaps™ finally make trusted, remote identity verification possible. As the only technology backed by a persistent spoof bounty program and NIST/iBeta Certified Liveness Detection, FaceTec is the global standard for 3D Liveness and Face Matching with millions of users on six continents in financial services, border security, transportation, blockchain, e-voting, social networks, online dating and more. www.facetec.com

Oz Forensics

Oz Forensics is the independent private vendor of robust, technology-based, and AI-powered liveness detection and face-matching solutions founded in 2017 and headquartered in Dubai, UAE. We confirm the security level of our solution by certifying the ISO-30107 Level 1 and 2 standards. https://ozforensics.com/

AUTHENTICID

AuthenticID provides 100% automated identity verification and fraud detection solutions that are leveraged by companies worldwide, including 2 of the top 3 U.S. Banks, 8 out the top 10 wireless providers in North America, and 2 of the 3 credit bureaus. Using proprietary computer vision and machine learning technology, these solutions help companies accurately verify the identity of their users across retail, digital and call center environments for onboarding and ongoing re-authentication events; KYC, IAM, and more. The solutions are easy to integrate and provide customers a large ROI by stopping fraud losses,

Related News



Identity News Digest – August 15, 2024


Identity News Digest – May 17, 2024


ID Tech Digest – January 27, 2025


ID Tech Digest – January 16, 2025


ID Tech Digest – October 29, 2024


Dubai Cuts Cruise Ship Immigration Screening by 20 Mins with Facial Recognition Tech

Filed Under: Features, News, Podcasts
Tagged With: 2D vs 3D facial recognition, 3D biometrics, biometric liveness detection, Biometric Security, cryptographic data security, digital identity, FaceTec Jay Meier, FaceTec technology, facial recognition, identity management, spoofing prevention, UR Code protocol

increasing customer conversion at onboarding, reducing operational costs and allowing quick and cost-effective operational scalability, all while ensuring global privacy regulations are complied with.
https://www.authenticid.com/

Lakota
SOFTWARE SOLUTIONS

Founded in 2007, **Lakota Software Solutions** is an American company with a world-renowned reputation for developing robust biometric software and systems. Our vendor-agnostic products are tailored to ensure compliance with ANSI/NIST-ITL standards and EBTS specifications, facilitate seamless integration with other biometric systems, and optimize accuracy, cost-effectiveness, and scalability. https://lakotasoftware.com/

IDENTITYWEEK
GLOBAL • TRUSTED • VISIONARY

Identity Week aims to be a significant identity industry catalyst. It's our mission is to help accelerate the move towards a world where trusted identity solutions enable governments and commercial organisations to provide citizens, employees, customers and consumers with a multitude of opportunities to transact in a seamless, yet secure manner. All the while preventing the efforts of those intent on doing harm. https://identityweek.net/

The Prism Project

The Biometric Digital Identity Prism is a market landscape framework designed to help influencers and decision makers understand, innovate, and implement digital identity technologies and solutions. This innovative framework for understanding and evaluating the rapidly evolving biometric digital identity marketplace is the only market model that is truly biometric-centric based on the foundational conviction that in the age of digital transformation the only true, reliable link between humans and their digital data is biometrics. https://www.the-prism-project.com

RECENT POSTS

AI Update: National Security, Tariffs, and a $20B Startup Without a Product
ID Tech Digest – February 7, 2025
Sacramento International Airport Launches Mobile Driver's License Verification at TSA Checkpoints
Credivera Acquires Oliu Technology Stack from ATB Ventures, Expanding IDV Capabilities
Yuno Launches Mastercard Payment Passkey Service in Latin America

BIOMETRIC ASSOCIATIONS

ibia
fido alliance member

About Us
Company Directory
Advertise With Us
Contact Us
Privacy Policy
Terms of Use
Archives
CCPA: Do not sell my personal info.
FOLLOW US
Copyright © 2025 Verse Media
Could not connect to the reCAPTCHA service. Please check your internet connection and reload to get a reCAPTCHA challenge.

https://web.archive.org/web/20230316184525/https://dev.facetec.com/configuration-options

INTERNET ARCHIVE WayBackMachine https://dev.facetec.com/configuration-options Go JAN MAR APR 16 2021 2023 2024 About this capture
6 captures 15 Jan 2021 - 10 Jan 2026

Architecture: Features & Configuration Options

The FaceTec Server Software runs 100% in YOUR Private Cloud inside YOUR firewall. None of your users' PII or Biometric Data is sent to FaceTec.

Device SDK Features & Options

Compare the Device SDK properties for the 3D Liveness Check & 3D Face Verification use cases.

FaceTec Device SDK Features	3D Liveness Check (No Face Matching)	3D Face Verification (Matching + Liveness ✓)
Device Compatibility	Android, iOS, Mobile Browsers, PWA & PC w/Webcam	Android, iOS, Mobile Browsers, PWA & PC w/Webcam
Biometric Data Stored	None, or On-Server (for Audit Trail)	Encrypted FaceMap Stored on Server
3D Liveness Verified	Yes, On-Server	Yes, On-Server
3D Face Match to Govt. Photo ID	Yes, with Photo ID Identity Check	Yes, with Photo ID Identity Check
3D Face Matching	Not Applicable	On-Server - 1:1 & 1:N (1/125M FAR @ <1% FRR)
Device SDK Download Size	iOS/Android: 3.9MB & Browser: 3.7MB	iOS/Android: 3.9MB & Browser: 3.7MB
Transmitted 3D FaceScan Size	~350KB	~350KB
Age Check (Anonymous)	Yes, on 3D FaceScans/Maps & 2D Images	Yes, on 3D FaceScans/Maps & 2D Images

Testing API vs. Customer Hosted & Run Server SDK

Compare the Server SDK properties for the FaceTec Testing API & Customer Hosted Server SDK when in Production.

Features & Options	FaceTec Testing API	Customer Hosted Server SDK/API
At Rest/In Transit Data	Encrypted	Encrypted
Biometric Storage	FaceTec Testing Cloud (AWS)	Customer's Private Server / Cloud or User Device
Server/Cloud Software Required	None (all operations REST API based)	FaceTec Server SDK (provides private REST API)
1:N De-Duplication Check	For Testing/POC Only	Yes, new users can be checked for dupes
Migration to the Other API	Yes, move from FaceTec's Managed Testing API to your own Server SDK/API w/ a Device SDK Update	Not Applicable
Server Sample Code & Demo Apps	Yes, via REST API	Yes, Java, Docker
Startup Effort	Sample apps pre-configured for immediate testing	FaceTec Server SDK deploys quickly
Pricing Model	Free, For Initial Setup & Testing Only	Billed Per 3D Liveness Check Session/User

Standard Server SDK vs. Custom Server SDK

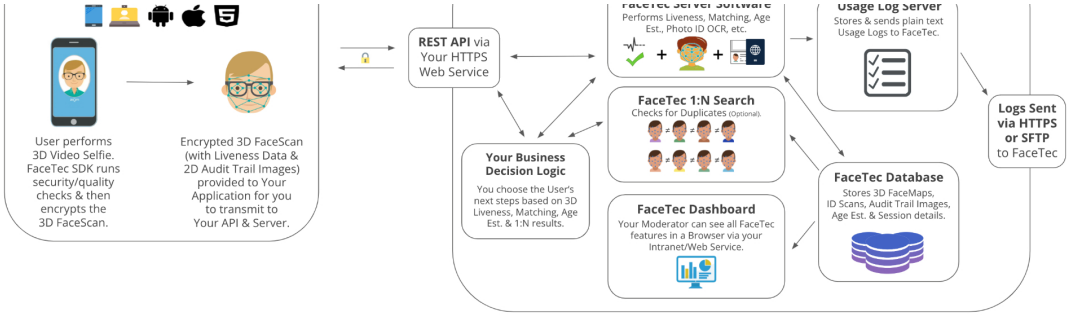
Feature comparison of Standard Server & Custom Server SDKs.

Customer Hosted Server SDK Features	Standard Server	Custom Server
Server Dashboard (only visible to Customer)	Available by Default	Available by Default
Databases Supported	In-Memory Stub DB, MongoDB, DocumentDB, and S3	Any. Customer configured (examples provided).
Startup Effort	1 Config File with several properties	Initial development deploys in minutes. Customer can customize and configure the REST API code.
Customization Level	Closed Application	Customizable REST API code provided
Uses Server Core	Yes	Yes
Difference in 3D Liveness or Matching Accuracy	None, uses same Server Core Library	None, uses same Server Core Library

Private Cloud Architecture & Data Flow

High-level overview of how 3D FaceScan data and ID Scans flow from your users' devices to your Private Cloud.





Notes on Architecture & Data Privacy

- FaceTec does NOT provide a biometric data processing service. FaceTec is software that You download, integrate, and run inside your Private Cloud.
- First, you download FaceTec's device-side user SDKs and integrate them into your Apps & Webpages.
- Second, you download FaceTec's server-side software and you configure it inside Your Private Cloud, inside Your firewall.
- Once in production, with permission from the user, your App/Webpage collects the user's 3D FaceScan (and/or Photo ID Scan data).
- The 3D FaceScan data is sent from the user's device **directly** to your Private Cloud for processing by the FaceTec software (that **You** run on **Your** Private Cloud/Servers).
- The Liveness-proven 3D FaceScans/Maps can then be stored on Your Private Cloud (never FaceTec's servers), and you can delete them at will.
- NONE of your Users' Biometric Data or User PII is sent to FaceTec when the software is deployed with your actual users.
- No FaceTec software feature (KYC/IDV Dashboard, Database, 1:N Search, or any other feature) requires any user biometric data or PII to be sent to FaceTec.

Hardware/Performance Example

Private Cloud Server Configuration: Cluster of 4 Servers running 8 or 16-core Intel Xeon Platinum 8000 Series CPUs
RAM for each Server: Number of CPUs * 2.5 GB of memory/RAM (e.g. an 8 CPU system has 20 GB of RAM; a 16 CPU system has 40 GB of RAM)

- 1.5+ million Liveness Checks per day (depending on configuration).
- 1:N Search for duplicates in a Database of 1,000,000 3D FaceMaps can be performed in under 1 second.
- On AWS/Google the cost for four 8 or 16-core machines is ~$4K - $10K annually.
- Other additional costs to consider: 3D FaceMap storage, database for transaction logs & analytics.

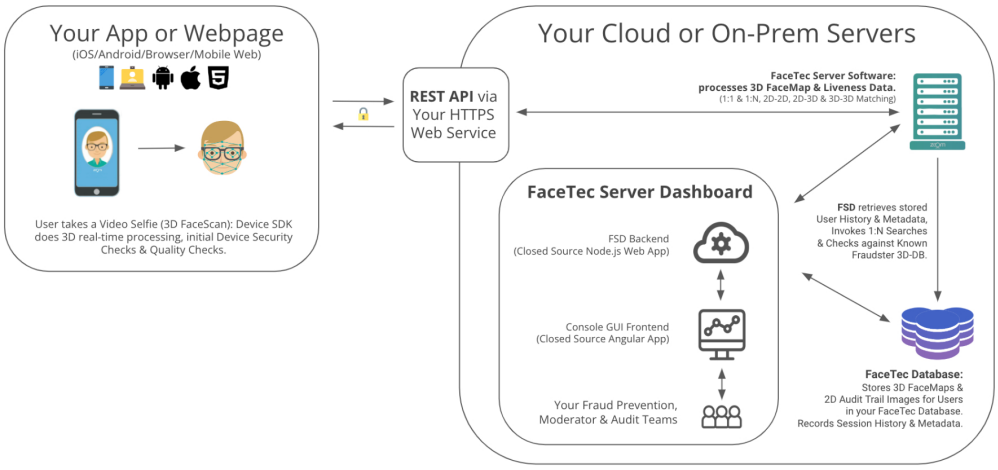
> **CPU Compatibility Note**: Please use Intel Xeon Platinum CPUs for your Server SDK instances. FaceTec leverages specialized Intel functionality for significantly optimized performance. AMD, ARM, or other non-Intel Processors are not recommended and not supported, and will lead to slow performance, or other issues.

Calculating Your Infrastructure Requirements

- To double the requests/sec OR the geographic regions, multiply the required hardware by two.
- To be resilient to load spikes, use auto-scaling for your hosted FaceTec Server with a service like AWS Elastic Beanstalk.

Server Dashboard & Compatibility

The FaceTec Server Dashboard (Video Tour Here) shows FaceTec usage from your users as they perform 3D Liveness Checks, Enrollments, Verifications, Photo ID Matches, & Age Checks. Try the Developer Testing Dashboard Here.



FaceTec Server Software Dashboard

- Hosted 100% inside Your Firewall through Your Private Cloud or Your On-Premise Servers.

- Visible only to the internal staff you designate and never to FaceTec staff.
- You secure the FSD Web App (internal access controls, whitelists, etc.)
- Closed-source Web App → You perform updates as FaceTec improves its software.
- Must use FaceTec Server Managed SDK.
- Databases supported: MongoDB/DocumentDB/CosmosDB.
- Planned database support: SQL, Dynamo, MySQL/Aurora, & more.

© 2023 FaceTec, Inc. · Multiple US & International Patents Granted · All Rights Reserved
Terms & Conditions. · Site Privacy Policy. · SDK Privacy Policy.