

NIST 800-63-4: Request For Information - Reply

Introduction - FaceTec, Inc. (a Delaware Corp.) is the leading global 3D face liveness and matching software provider for Remote Identity platforms. U.S. federal Agencies, U.S. States, numerous foreign/sovereign governments, and hundreds of commercial entities use FaceTec's technology to verify and authenticate citizens, customers, and users. For example, Utah and Colorado incorporated FaceTec in their mDL programs, and the Department of Homeland Security has incorporated FaceTec's technology into Mobile Trusted Traveler-related programs.

Hundreds of millions of users worldwide have proven their liveness remotely with FaceTec on tens-of-thousands of different smartphone, tablet, and webcam models (mostly low-end & low-resolution), and with no observable age, gender, or skin-tone bias. **FaceTec will conduct well over one billion 3D Liveness checks in 2023 and has seen a 100%-plus annual growth rate for the last three years.** In addition, **FaceTec is the only liveness and biometric vendor that operates a persistent Spoof Bounty Program**, offering as much as \$600,000 to incentivize hackers to attempt to bypass the biometric cybersecurity platform. FaceTec software has successfully defended against over 130,000 Bounty Program attacks, providing unmatched experience rebuffing today's most sophisticated threats.

FaceTec agrees with NIST's decision to require all IAL2 sessions in unsupervised, remote identity proofing scenarios to have liveness-proven biometric data positively match previously stored and trusted biometric data for that individual. However, biometric matching against various identity documents creates significant vulnerabilities. Fake identity documents, virtually impossible to detect, are available on the dark web, often including stolen legitimate identity data (that the issuing authority will verify is not synthetic) beside an image of a fraudster's face. Unless tampered document validation is 100% accurate, which is highly unlikely with user-provided documents, the CSP might bind the fraudster's face to the stolen identity and then routinely authenticate that fraudster as the identity theft victim. Therefore, FaceTec strongly recommends matching the Claimant's liveness-proven 3D face data to the 2D face image on file at the Issuing Authority before binding the user to the Subscriber Account.

Further, SP800-63B-AAL1, AAL2, and AAL3 appear only to verify the presence of an expected/trusted device but do little to authenticate the physical presence of the legitimate Subscriber. An unauthorized person can control any authenticator not derived directly from the physical human Subscriber. Thus, all human authentication is probabilistic. Combining deterministic and probabilistic calculations produces only probabilistic outcomes. Thus, all remote human authentication in a *digital identity* scheme is probabilistic. Since biometrics is the only authenticator derived directly from a verified human being, liveness-proven biometrics provide the highest possible authentication confidence. Consequently, FaceTec recommends requiring liveness-proven biometrics to achieve AAL2 and AAL3.

Server-side liveness confirmation upon enrollment is critical. CSPs should collect liveness and biometric matching data concurrently. When possible, the data should overlap. FaceTec strongly recommends binding the Claimant's Liveness-proven biometric data to the verified Subscriber Account and matching new Liveness-proven data against it in every subsequent authentication session.

In the following pages, FaceTec thoroughly describes known threat vectors, explains the risks of biometric spoofing and camera bypasses, and suggests numerous procedural recommendations that will significantly increase the security of these systems.

Thank you for the opportunity to contribute FaceTecs knowledge to NIST 800-63.

FaceTec's Recommendations to SP800-63A:

Sect. 4.2 - General Requirements: The CSP SHALL perform a Liveness check when collecting biometric data.

Sect. 4.2 - General Requirements: The CSP SHALL bind collected biometric data to the Subscriber Account.

Sect. 5.2.1: The CSP SHALL perform a Liveness check when collecting biometric data.

Sect. 5.2.2: The CSP SHALL perform a Liveness check when collecting biometric data.

Sect. 7: The CSP SHALL perform a Liveness check when collecting biometric data.

FaceTec's Recommendations to SP800-63B:

Sect. 4.1.3: Reauthentication: Any biometric systems used for Subscriber reauthentication SHALL perform a Liveness check on the data collected before matching during any subsequent authentication.

Sect. 4.2.1:AAL-2 and Sect. 4.3.1:AAL-3: The CSP SHALL use newly collected liveness-proven biometric data to match trusted data for Subscriber authentication.

Sect. 4.2.3 and 4.3.3: Reauthentication: Any biometric systems used for Subscriber reauthentication SHALL perform a Liveness check with subsequent authentication.

Sect. 5.2.3: Biometrics: All biometric systems SHALL include Liveness Detection (Camera/Sensor Bypass detection and PAD capabilities). All biometric data used in matching for Subscriber Authentication SHALL be compared to trusted biometric data previously bound to the Subscriber Account. Any biometric systems used for Subscriber authentication SHALL perform a Liveness check on the data collected before matching during subsequent authentication.

Sect. 5.2.3: Biometric Reauthentication: Any biometric systems used for Subscriber reauthentication SHALL perform a Liveness check on the data collected before matching during subsequent authentication.

Sect. 6.1.1: Binding: All biometric authenticators SHALL compare claimant biometric data to biometric data previously bound to the Subscriber Account.

Sect. 6.1.2: Biometric data bound to a device SHALL NOT constitute the binding of biometric data to a Subscriber Account.

ID Proofing: Matching 2D Photos to 3D People at Varying Distances

Despite our innate human ability to correlate them to a natural person, 2D photos are not true, accurate, or consistent representations of a 3D human face. 2D Photos are convenient derivatives that are, unfortunately, highly affected by pose, angle, capture distance, and lighting. The human visual cortex can leap from 2D photos to 3D faces much better than AI because the human brain has evolved to store 3D models of familiar objects, surroundings, and people. However, that innate ability falsely leads to the incorrect human bias that 2D photos are consistent representations of 3D humans. For example, a to-scale 3D sculpture is a much more accurate representation than any 2D photo could ever be. The sculpture can be viewed from any angle in 3D space; with it, any photo of the subject can be substantially recreated.



©Stephen Eastwood 2008

Government ID Photo-distance



©Stephen Eastwood 2008




Selfie-distance



2D photos captured at government ID photo distance versus selfie distance for the same person are very different, and modern 2D:2D Photo Matching systems rarely provide accuracy above 1/10,000 FAR at a <1% FRR in these scenarios with real-world devices. However, capturing 3D data increases accuracy by orders of magnitude and enables higher match confidence. Moreover, AI-based 3D algorithms can compensate for image capture distance variability and extrapolate how the face should appear at various capture distances, increasing 3D:2D accuracy to 1/2,000,000 FAR @ <1% FRR. Age, gender, or ethnicity biases are minimized while preventing Passport Photo Morphing and other Substitution Spoof frauds.

Liveness.com - Presentation Attack & Camera Bypass Threat Vectors

In 2001, Dorothy Denning, Ph.D., of the [National Cyber Security Hall of Fame](#), coined the term "Liveness" and stated that "[It's "liveness," not secrecy, that counts.](#)" More insights from Ms. Denning, and more info about biometric security in general, can be found on [Liveness.com](#).

The below attack vector/threat levels correspond with and expand on the artifact types described in ISO-30107-3 from 2017. However, ISO 30107-3 did not contemplate Deep-Fake videos, Puppets, or Camera Bypasses, so any testing that *only* considers threats outlined in ISO-30107-3 is no longer adequate ([attack example](#)) to ensure any level of Liveness security.

Artifact Level	Description	Example
Level 1 (A) (Spoof Bounty Avail)	Hi-res paper & digital photos, hi-def challenge/response videos and paper masks. Beware: iBeta Lab Tests DO NOT include digital deepfake puppets, but FaceTec's Spoof Bounty DOES include deepfake puppets.	
Level 2 (B) (Spoof Bounty Avail)	Commercially available lifelike dolls, and human-worn resin, latex & silicone 3D masks under \$300 in price.	
Level 3 (C) (Spoof Bounty Avail)	Custom-made ultra-realistic 3D masks, wax heads, etc., up to \$3,000 in creation cost. *No Lab Testing Avail	

Bypass Level	Description	Example
Level 4 (Spoof Bounty Avail)	Decrypt & edit the contents of a 3D FaceMap to contain synthetic data not collected from the session, have the Server process and respond with Liveness Success.	
Level 5 (Spoof Bounty Avail)	Successfully take over the camera feed & inject previously captured frames that result in the Server responding with Liveness Success.	

dev.facetec.com/spoof-bounty-program

- Threats against today's remote identity proofing processes:
 - Presentation Attacks performed by a bad actor showing a mask, mannequin, video, digital, or paper photo (synthetic artifact) instead of a real, 3D human's face. These attacks can affect initial Identity Verification *and* future Authentication sessions. Presentation Attacks are among the easiest to attempt and are pervasive, with an estimated 2% of all current Remote ID Verification attempts being PAD attacks. While often simple to procure and perform, Presentation Attacks can be challenging to detect and are considered Levels 1-3 on the [Liveness.com](https://liveness.com) Attack Vector Scale.
 - Biometric Template Tampering Attacks are performed on the device, where the subject's biometric data is replaced in the legitimate user data with imposter data before being matched against trusted data, or "man-in-the-middle" attacks, where the payload is intercepted and replaced in transit to the server. These attacks are considered Level 4 on the [Liveness.com](https://liveness.com) Attack Vector Scale.
 - Camera Bypass Attacks include processes whereby the bad actor bypasses the camera hardware and injects previously collected data into the video feed. Common Bypass techniques include using virtual camera software (e.g., [ManyCam](https://www.manycam.com)) or leveraging vulnerabilities in WebRTC by setting injection points or running the application on an emulator. These attacks are considered Level 5 on the [Liveness.com](https://liveness.com) Attack Vector Scale.
 - "Imposter" Attacks are perpetrated by presenting a live human to the camera who looks similar to the legitimate user. These attacks are often successful against 2D or otherwise weak matching algorithms incapable of compensating for image capture perspective distortions. In addition, 2D "Selfie-to-ID Card" systems are particularly vulnerable to perspective distortions and result in lower match confidence. Lastly, 2D matching technologies or techniques that rely on collecting color hue are inherently less accurate when authenticating dark-skinned, young, and female users, while 3D systems that do not depend on hue are not.
 - In-Device Authentication Spoof Risk - Remote Identity Proofing and Authentication systems relying on biometric matching on a mobile device (like Apple and FIDO) are vulnerable to Imposter Attacks for several reasons. First, the enrolled biometric data on the device is anonymous and cannot be bound to a Subscriber Account. Second, the enrolled data cannot be moved from the device to a server, limiting match data size to accommodate fixed and limited in-device processing capability, impacting potential accuracy. Further, in-device biometric processors do not allow scanning for duplicate or fraudulent identity profiles (i.e., "de-dup") within an identity profile database. As a result, in-device biometric sensors are particularly vulnerable to Level 1-5 attacks on the [Liveness.com](https://liveness.com) Attack Vector Scale.
- Liveness methods used by identity proofing and technology providers:
 - Active Liveness Detection commands the user to successfully perform a movement or action like blinking, smiling, tilting the head, and track-following a bouncing image

on the device screen. Instructions must be randomized, and the camera/system must observe the user perform the required action.

- Passive Liveness relies on involuntary user cues like pupil dilation, reducing user friction and session abandonment. Passive liveness can be undisclosed, randomizing attack vector approaches. Alone, it can determine if captured image data is first-generation and not a replica presentation attack. Moreover, within specific system architectures, it can determine if the user is present in real-time, eliminating Levels 4-5 Attacks like video injection and others.
 - Device & Server-Side Liveness - Significantly higher Liveness and biometric match confidence can be gained if device camera data is captured securely with a verified camera feed and the image data is verified to be captured in real-time by a device SDK. Under these circumstances, Liveness and Match confidence can be determined concurrently from the same data, mitigating vulnerabilities.
 - Multimodal Liveness utilizes numerous weak Liveness modalities to establish user choice and increase the number of devices supported. Unfortunately, this often creates user interaction friction, requiring the user to "jump through hoops" of numerous Active Liveness tests.
 - Liveness and 3D Depth Data Dependence - A human must be 3D to be alive, while a mask-style artifact may be 3D without being alive. Thus, while 3D face depth measurements alone do not prove the subject is a live human, verifying 2-dimensionality proves the subject is not alive. Regardless of camera resolution, 3-dimensionality provides substantially more usable and consistent data than 2D, dramatically increasing accuracy. Therefore, 3D depth detection is a critical component of stronger Liveness Detection. Importantly, deleting used Liveness data is an effective means of mitigating Honeypot risk.
1. Specialized In-Device 3D Camera Hardware (i.e., Apple's Face ID) can collect 3D Face Data almost instantaneously by projecting invisible dots on the face and analyzing derived depth data. However, it requires special hardware but provides much higher accuracy than legacy 2D Matching.
 2. 3D Face Data Collection Software utilizes video frame data captured from the X & Y axes from numerous 2D video frames over a few seconds, and processes observed changes in the facial appearance to "reverse-engineer" the 3D Face. 3D Face Liveness software systems can securely deliver interdependent, concurrent Liveness and biometric data to a server for authentication against the Subscriber Account and other subscriber accounts (1:N) for de-duplication and other anti-fraud tactics.
- Relevant standards and testing/certification programs for these types of technologies:

- [ENISA Remote ID Proofing Report](#) - Published: March 2021 - "1. During the identity verification session, the "liveness" of the applicant's facial image is verified. Presentation attack detection (PAD) and face-matching controls are used. The technology addresses various presentation attacks (e.g., still or video imagery submission, usage of high-quality masks, a replay of a previous video capture). The system is continually monitored and reacts to evolving threats. Face matching algorithm uses the latest advances in deep neural networks to deliver matching performance with the highest level of assurance. It is optimized for 'selfies' taken on smartphones and PCs in a huge variety of lighting conditions, poses, and facial features."
 - [ETSI "Survey of technologies and regulatory requirements for identity proofing"](#) Published: March 2021 - "...the applicant to take and send a mobile phone video or photo with other liveness checks; compare the applicant's submitted photo to the photos on the passport identity evidence or the photo on file in the government's passport or license database."
 - [Liveness.com](#) - Published: September 2020 - Threat Vector Scale: PAD Levels 1-3, Level 4 = Payload Tampering Prevention & Level 5 = Camera Feed Bypass Prevention
 - [ISO 30107-3](#) - Published: 2017- Purely Presentation Attack Detection Levels 1-3, no cybersecurity aspects or bypasses addressed.
- The impact of Liveness Detection or other Presentation Attack Detection capabilities on cost, usability, and market availability:
 - **Bias:** Liveness Detection *hardware* is expensive, largely proprietary, not interoperable, and limited in functionality and distribution. It can be economically biased against the less affluent. Liveness techniques that rely on typical commercial camera sensors to capture reflected light from human skin are inherently biased against certain skin tones, age, and gender. Conversely, 3D *software* is inexpensive and easy to deploy, improve, and maintain while mitigating economic, skin, age, and gender biases.
 - **In-device Limitations:** Most in-device liveness and biometrics, like Apple's Face ID and FIDO Authenticators, preclude server-side processing, limiting processing capability to that of the device processor and limiting potential accuracy. They cannot authenticate to a Subscriber Account or Issuer's root identity database for de-duplication and other anti-fraud strategies.
 - **Friction & Abandonment:** Multimodal Liveness and matching tend to aggregate weak Liveness systems, dramatically increasing cost, session duration, user friction, and session abandonment. It doesn't significantly increase matching accuracy in most use cases, and it eliminates the opportunity for Liveness and match test concurrence, which limits potential confidence.
 - **Active vs. Passive:** Active and Passive Liveness techniques are vulnerable to various and potentially different spoofing vectors. Passive Liveness looks for signs of

- “Deadness” and involuntary human Liveness signals, while Active Liveness primarily looks for the user to respond to a command for movement. Active Liveness systems increase friction and session abandonment and are more vulnerable to attack vectors like deep fake/video puppets or Imposter Attacks.
- **3D vs. 2D:** Three-dimensional (3D) Liveness approaches are able to capture orders-of-magnitude more data, increasing security confidence. They also are less reliant on light reflective or refractive techniques and are, therefore, naturally less biased toward skin tone, age, and gender. 2D systems are inherently less accurate than 3D and vulnerable to perspective distortions related to variable capture distances.
 - **Backward Compatibility:** 3D Liveness software approaches inherently collect orders-of-magnitude more biometric Liveness and Matching Data from the same 2D camera and are significantly more backward compatible with old devices than 2D.
 - **Honeypot Risk:** Requiring the collection of 3D Facial Liveness and Matching data concurrently from the same video frame data feed can mitigate honeypot risk. By deleting some liveness data not required for 3D matching after the initial Liveness check (one half of the “key”), the remaining 3D Face Matching Data, even if stolen and decrypted, cannot alone be re-submitted successfully. Yet, the 3D Matching Data can remain stored in the database for subsequent user authentications or account recovery.
 - **Cost Reduction:** 3D software approaches also reduce costs significantly. They do not require specialized hardware, specific device brands, cameras, camera resolution, or operating systems. They can also utilize server-side matching, enrolled profile data, and server-side binary API responses.