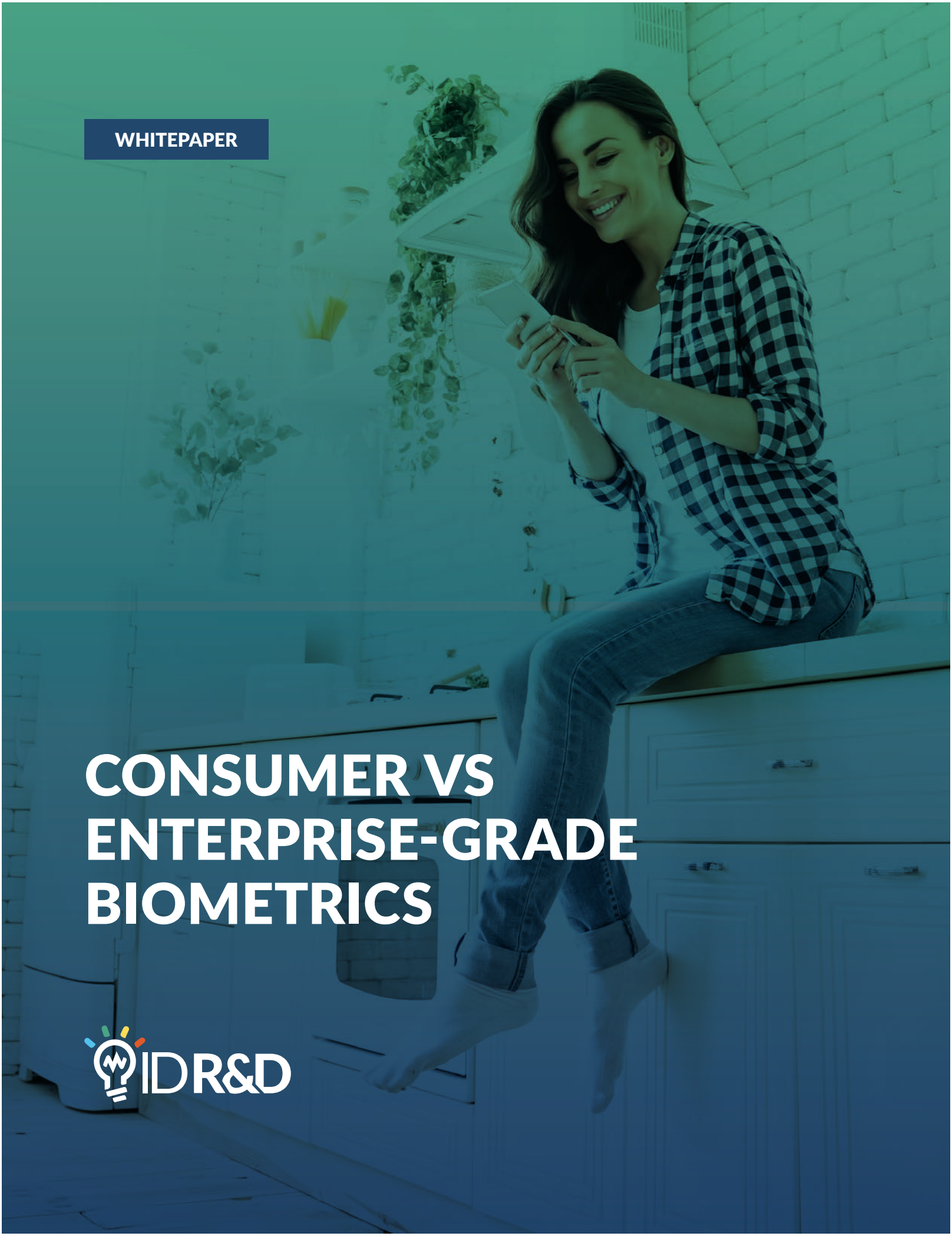


WHITEPAPER

CONSUMER VS ENTERPRISE-GRADE BIOMETRICS

IDR&D

INTRODUCTION

Biometrics, the ability to determine an identity based on some measured characteristic of a person, have progressed from a novelty to a commonly used capability thanks to Apple, Samsung, Google, and others who introduced fingerprint, face, and sometimes iris biometrics technology into their mobile devices. Apple also recently announced the planned addition of Touch ID and Face ID to its Safari browser. These biometrics are inextricably part of the consumer's device, thus the term "consumer-grade" biometrics.

Many enterprises rely on consumer-grade deployments to enable their customers to bypass the normal login process in the company's mobile app. But do these consumer-grade biometrics provide the level of security enterprises need to fight fraud, protect customers, and manage risk? In order to take control of user authentication and to achieve higher levels of security while also gaining the advantage of lower friction in the customer experience, enterprises must deploy **enterprise-grade biometrics.**

This paper explains the key differences between consumer-grade and enterprise-grade biometrics and why using the former exposes companies to a false sense of security and greater risk.

WHAT ARE CONSUMER-GRADE BIOMETRICS?

It is reported that the average smartphone owner unlocks their phone 150 times a day. Users aren't willing to type a passcode 150 times a day. So they leave the phone unlocked for longer periods of time, which is a security risk. To alleviate the friction of typing passcodes, mobile device manufacturers added biometrics. This was a smart move because the biometrics enable convenience and close the security loophole of leaving the phone unlocked.

However, it is critical to note that these device-based biometrics, whether finger, face, iris, or other, are just options to unlock the device instead of typing a passcode. They are a substitute for the passcode, not an additional factor on top of the passcode. They do not add security, only convenience. Whoever controls the passcode can easily enroll their biometrics on the device.

Today, it is common for enterprises to use the device's embedded biometric capability that unlocks the device to also bypass the normal bank login and password. For example, on an iPhone 7, which has fingerprint biometrics but no face biometrics, many banks allow customers to use Touch ID to login to their mobile application. As a user, it's nice to skip the login and password and simply touch the home button.

Herein is the limitation of the consumer-grade biometric. The bank is making a leap in assuming that if you successfully login to the device with a passcode and successfully set up a biometric, then after logging into the bank app with a username and password at least one time, you are likely the person who set up the banking app. The biometric provides a substitute for a login on the device and an approximate login substitute for the mobile application. This leap of faith is the risk the bank is willing to take to enable convenience when accessing the app.

To restate this important point, the on-device consumer-grade biometric does nothing to provide greater protection for the enterprise application; it only serves to make the login experience on the enterprise's mobile app more convenient.

Enterprises can do better. ***Enterprise-grade biometrics provide both superior security and superior convenience.*** The next section dives deeper into how.

© 2020 ID R&D

ENTER ENTERPRISE-GRADE BIOMETRICS

Enterprises are only now beginning to leverage biometrics beyond consumer-grade capabilities. They do so by deploying biometrics directly within the enterprise mobile application, providing an authentication factor **separate** from the device. The result is far stronger security while also gaining convenience in the user experience, leading to a truly passwordless customer journey. Enterprise-grade biometrics **are biometrics which enterprises deploy in the application and do not rely on the specific device.**

Enterprises gain distinct security and user experience advantages by deploying within the application rather than relying on consumer-grade biometrics. The following table illustrates the top five differences.

© 2020 ID R&D

CONSUMER-GRADE	ENTERPRISE-GRADE
Consumer chooses the biometric With consumer-grade deployments, the enterprise must accommodate the consumer's choice of security options, ranging from no biometrics at all to high-end, multi-camera options based on the consumer's choice of device. The consumer also determines the quality of the biometric, usually unwittingly, as different manufacturers use different components. As a result, the enterprise has zero control over the biometrics yet carries all of the liability should the enterprise allow them to be a proxy for a mobile app login.	**Enterprise chooses the biometrics and controls the security level** With enterprise-grade biometrics, the enterprise decides how and when to apply biometrics as a factor in the authentication process because the biometric is built into the enterprise system and mobile application. Consequently, the enterprise has the power to enforce the same security level and user experience whether the device is low-end or high-end.
Equivalent to a login on a device On-device, consumer-grade biometrics enable the convenience of not needing to login to the device with a password. This is equivalent to confirming the device as a factor for authentication -- e.g. the "something you have" factor[1]. If you can unlock your device, it's the same device you have been using, and it is not reported stolen, it's likely that you are the rightful owner. If a user upgrades or changes their device, they need to re-enroll their biometrics.	**Provides a true authentication factor** Biometrics included within the enterprise application function independently of the device, which in turn means that the biometric is a true factor. This "something you are" factor is in addition to knowing that the user has possession of the device, the "something you have" factor. Furthermore, by using multiple biometrics, the biometric factor becomes even stronger, giving the enterprise the flexibility to combine biometrics or to dynamically implement step-up authentication to manage varying risks and attack vectors. If the consumer changes a device, there's no need to re-enroll their biometric. Instead, the biometrics remain a true, independent factor **regardless of the device.** This becomes a powerful tool for preventing fraud attacks.

© 2020 ID R&D

CONSUMER-GRADE	ENTERPRISE-GRADE
Does not protect against common attacks The most common type of attack related to customers in an enterprise, particularly banking, is an account takeover attack. Criminals use social engineering or hacking to steal login IDs and passwords to the banking application, the "something you know" factor. Then, to circumvent the device being used as a second factor, they falsely inform the enterprise that their device has changed. Because consumers eventually change devices, the bank needs to distinguish between the valid consumer and a criminal. Consumer-grade biometrics do nothing to assist in validating the consumer on a new device. Instead, the bank has to revert to other means to prove the identity of the customer.	**Defends the enterprise from Account Takeover attacks and fake account setup** A direct consequence of the fact that enterprise-grade biometrics provide an independent factor is that the biometrics provide a mechanism to confirm an identity, even on a new device. And because this is a high risk event, the enterprise can choose to use multiple biometric modalities to increase confidence while maintaining very low friction in the user experience. Furthermore, a very important weapon against new account fraud is a watch list of known or suspected fraudsters. Enterprise-grade biometrics provide the ability to check new users against a watch list of repeat fraudsters; Consumer-grade biometrics do not.
Works only on the one device By definition, a biometric on a device is attached to that device. It is not stored or saved elsewhere, nor is it usable outside of the device.	**Works across communication channels** Consumers tend to interact with enterprises using the channel that best suits their needs, situation, and personal preferences. Enterprises therefore offer multiple channels, such as web, mobile, social media, and the call center. Enterprise-grade biometrics can be deployed individually or in combination to provide security across all of these channels. For example, an enterprise-grade voice biometric will work in the call center, web, mobile, and standalone channels like kiosks and ATMs.

© 2020 ID R&D

CONSUMER-GRADE	ENTERPRISE-GRADE
Limited to the performance of the device Manufacturers build devices with different ranges of hardware features and capabilities. A high-end device may have 3D cameras, infrared sensors, and plenty of image processing horsepower to run sophisticated algorithms. Low-end devices that reach many more people won't have these capabilities. Additionally, consumer-grade biometrics have factory-imposed settings that limit the enterprise's control over probability thresholds and the ability to balance false rejection and acceptance rates based on risk.	**Flexible performance with possibility to run the most sophisticated algorithms** While consumer devices have a broad range of processing power, there are minimum levels to make the device acceptable to the mass market. Unlike consumer-grade biometrics, enterprise-grade biometrics leverage this minimum capability while supplementing performance with back-end servers. For example, face recognition algorithms may run inside mobile applications with a relatively low penalty on application size. But it is also possible to use the device's camera, capture an image in the mobile application, and send a relatively small image of 100 kb or less to a server where powerful, GPU-based algorithms can process the image with far better effectiveness and speed than the processor on the device. With enterprise-grade biometrics, companies may dynamically determine how many biometric factors are needed, as well as probability thresholds for passing and failing based on risk. If the risk is high, for example, the enterprise can step up the authentication to two biometric modalities instead of one. A good example is the ease and simplicity of combining voice and face. Adding voice to face matching results in a solution that is 100 times more secure than face alone.

[1]Authentication systems rely on one or more factors out of three categories of actors to authenticate. These categories are generally known as "something you know," or knowledge-based authentication, like a secret password or details about you that others would not easily know; "something you have," such as a security token, fob, or device that belongs to you; or "something you are," such as your fingerprint, face geometry, iris pattern, or voice.

© 2020 ID R&D

ENTERPRISE-GRADE BIOMETRICS IN ACTION

Innovation in many industries often occurs with new challengers who re-think and disrupt the status quo. The same is true for biometrics in the enterprise. Most major banks, for example, operate in the world of consumer-grade biometrics and at best are betting on FIDO standards to achieve a second factor. New challenger banks have implemented and will be rolling out mobile-only banking in 2020 with enterprise-grade biometrics, rethinking and re-doing the user interface to simultaneously usher in higher security and greater convenience for their customers.

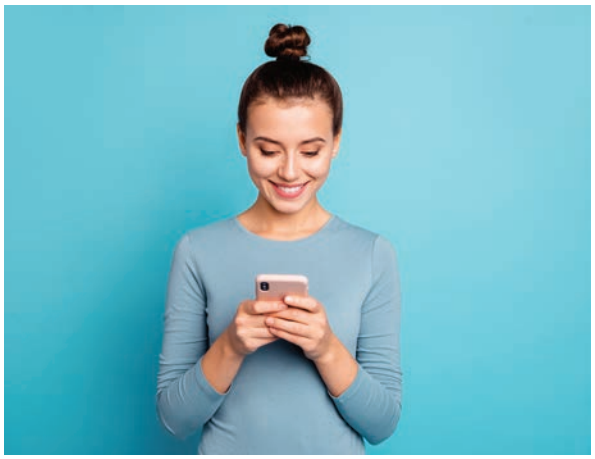
© 2020 ID R&D

ENROLLING CUSTOMERS IN AN ENTERPRISE-GRADE BIOMETRIC SOLUTION

Enrolling a customer in enterprise-grade biometrics is as fast or faster than typical enrollment for consumer-grade biometrics. Using voice and face, for example, enrollment requires recording a short passphrase three times for voice and taking one or two selfie images for face, both of which are protected by anti-spoofing to ensure a valid person is enrolling. For new customers, a best practice for the enterprise is to enroll the customer during onboarding, at the same time the consumer proves their identity for Know Your Customer (KYC) regulations. This approach enables one-time biometric enrollment across a wide range of current and future enterprise interaction points. Users never have to re-enroll when they get a new device.

KEEPING ENTERPRISE-GRADE BIOMETRIC DATA SAFE

Modern enterprise-grade biometric algorithms produce biometric templates that are not reversible or comprehensible by anything other than the software used to create the templates. Further encrypting these templates when stored renders stolen or hacked biometric templates beyond worthless. The enterprise may safely store the templates on the device and in the enterprise environment that adheres to industry information security standards. As a best practice, templates are never stored directly with personally identifiable information, only with a hash that links back to the identity.



© 2020 ID R&D

SECURE, FRICTIONLESS BIOMETRICS FOR THE ENTERPRISE

Enterprises are faced with the difficult task of strengthening security without sacrificing the user experience. Biometrics offer an accurate, convenient, and low effort way to authenticate customers. However, while consumer-grade biometrics deliver on convenience, they do not provide the security needed to protect the enterprise and its customers.

To learn more about our enterprise-grade biometric products and how we can help you deliver frictionless authentication, contact ID R&D at www.idrnd.ai