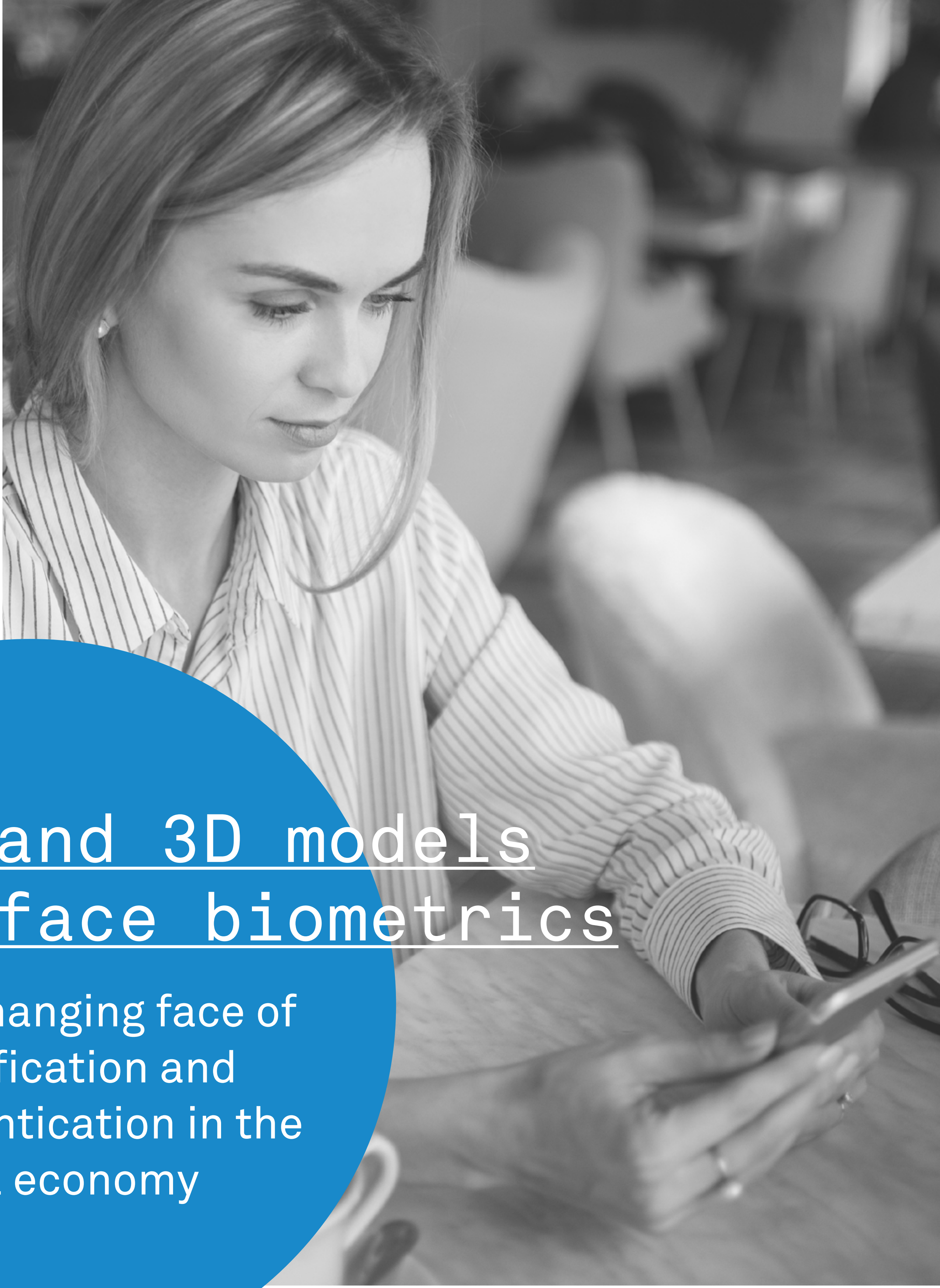

2D and 3D models of face biometrics

The changing face of identification and authentication in the digital economy

The article discusses:

- Global trends in consumer biometrics
- 2D and 3D models for face authentication
- How 2D and 3D face models impact liveness detection
- Considerations for implementing biometric solutions

Trends in consumer biometrics

Consumer biometrics is an emerging market, and it's promising to be a lucrative one. A 2018 report by Yole highlights four trends that speak to this potential:

- Total value of the consumer biometric market is predicted to grow from $4.8 billion in 2018 to $15.7 billion in 2023.
- In 2013, biometric hardware in high-end cellphones was mainly for fingerprint scanning and was valued at $5 per phone. In 2018, the hardware enabled fingerprint and face-based unlocking and authentication, and was valued at $15 per phone. By 2023, hardware is expected to accommodate fingerprint-, face-, retina- and voice-based biometric components, and be valued at $20 per phone.
- The CAGR for the consumer biometric sensors is expected to reach 20% from 2018 onward. Fingerprint modules are expected to hit 15%, while face-based biometrics are expected to reach 66% CAGR.
- Out of all biometrics, fingerprint/palm are predicted to still be the most used in 2023. 3D facial recognition is predicted to be a close second due to a marginally higher cost.

Biometrics are likely to influence payment, online identity and access management ecosystems in a way that changes the entire landscape of the digital economy. Because these technologies can identify an individual with great accuracy based on physical and behavioral attributes, they are being used more often for identification and authentication purposes.

Face-based authentication, especially 3D face modelling, is in line to play the biggest role in these changes. It will be the subset to watch in the coming years.

Biometrics for identification and authentication

Biometrics-based identification/authentication systems can be broken up into three groups: morphological, biological and behavioral.

The morphological segment drives the consumer biometrics market. Within this segment, facial recognition might be the most prominent, because face-based biometrics enhance our natural ability to recognize and distinguish human faces, while being non-intrusive, contactless, and socially accepted.

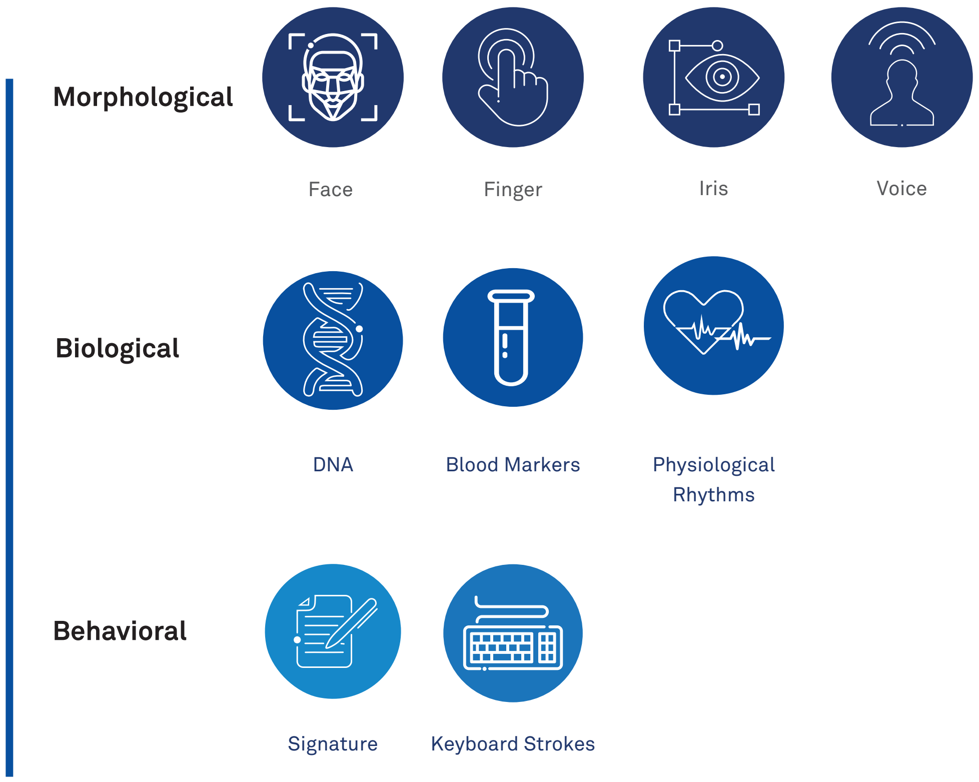

Figure 1 : Breakdown of biometrics-based identification/authentication systems.

Identification vs. authentication

Although there is a tendency, especially when referring to face biometrics, to use “identification” and “authentication” interchangeably, the two terms mean different things. Identification refers to the recognition of the user through image-matching. Authentication operates concurrently, but goes beyond identifying the user to also verify them as a real, live human.

Real-time liveness detection has become a necessity for authentication systems.

Face authentication systems: 2D and 3D face models

Biometric-based face authentication is a complex system. What’s referred to here is a simplified overview of that process.

There are two crucial steps in facial authentication process: registration and authentication. The user must register their biometrics (their face) with the system before their face can be authenticated.

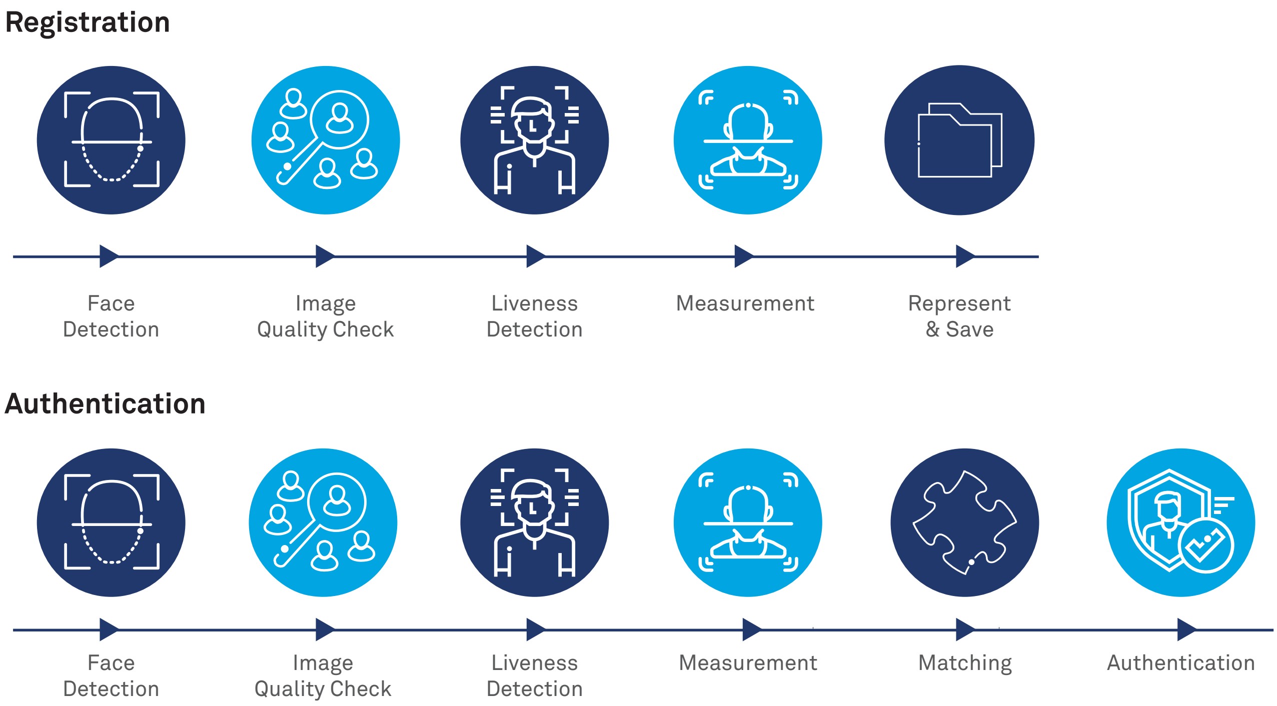

Figure 2: Overview of steps in face registration and face authentication processes.

Advancements in AI have enabled machines to detect numerous living human traits and characteristics, increasing the accuracy of biometric-based identification and authentication systems.

Similar technology is used for both authentication and identification, but the use cases and implementation details differ subtly. This paper focuses primarily on authentication-based systems, and how they are influenced by 2D and 3D imaging techniques.

Face Registration

Face registration is a 5-step process: face detection, image quality check, liveness detection, measurement, and representation (See Figure 2).

First, the system distinguishes the face from the background, followed by a quality check of the face’s image. Quality and efficiency of the registration process depend on variables like head position and light condition, so the system must perform various image quality checks. Because most systems work from a user’s device and are controlled by the user, variability in image quality is high. The system needs to be robust enough to understand a variety of input conditions, while only allowing the user to register if minimum criteria are met. At the same time, if image quality criteria are too stringent, user experience suffers, so there is a need for balance in this area. To strike this balance, some systems use intuitive screen-guides that make it easier for the user while ensuring the desired quality in the captured image.

Once the image has been captured and it meets the quality standards, the system then checks for liveness in the subject. This is a critical step for authentication, and we will explore it in detail in the next section.

The system then assigns nodal points to the various landmarks of the face image (raised and lowered points, edges, curves, angles). These nodal points are then measured and the system creates a face-print, which represents the human face and serves as an identifier.

There are two ways a face-print can be created using current technology: with a 2D face model or with a 3D face model. The 2D approach is based on information theory, and creates a model using the most relevant information presented on the surface of the face. In contrast, the 3D approach creates a facial geometry that represents the internal anatomical structure of the face, rather than the exogenous factors. Pure 2D models are sensitive to external factors like lighting conditions, head positions, facial expressions and makeup. 3D models are less affected by changes in external factors between registration and verification stages, but are computationally more intensive than 2D models.

The anatomical structure of an individual's face is relatively constant. It doesn't change much over time unless the individual undergoes a facial surgery that alters the anatomical structure. Because 3D models depend largely on the anatomical structure of face, they are more resilient with respect to time compared to 2D models. Such a timelessness of information is critical for authentication long after registration.

In the case of 2D models, systems extract a face model from a 2D image. For the 2D system to work, the head must be turned at least 35 degrees toward the camera. In a 3D system, an image of the face is taken using either a 3D camera or several images from a 2D camera. With 3D face models, systems focus on the distinctive features of the face where rigid tissue or bone is most apparent—the curves of the eye socket, the nose and chin—to identify the subject. These areas are all unique and do not

An important note on security

> The First IDentity Online Alliance (FIDO) is an open-industry association working to improve authentication by creating open standards that are more secure than passwords and SMS OTPs, simpler for consumers to use, and easier for service providers to deploy and manage. FIDO, with its members and liaison partners, has become a de facto standard in this space.
>
> In effort to ensure user privacy, FIDO compliance states that biometric data cannot be removed from the devices used to capture it. Additionally, FIDO protocols use standard public key cryptography techniques to provide stronger authentication. At the time of registration with an online service, the client device of the user creates a key pair: one private and one public key. The client device retains the private key and registers the public key with the online service. During authentication, the client device proves possession of the private key to the service by signing a challenge. The private key can be used only after it is unlocked locally on the device by the user. This local unlock can be accomplished by verifying a password, PIN, security key, fingerprint, face or voice biometrics etc.

depend on exogenous factors. Additionally, because 3D facial recognition uses depth and an axis of measurement, it is able to recognize a subject at different angles up to 90 degrees, a face in profile. With respect to face angle, 3D face models provide a distinct advantage over 2D models for practical user identification and authentication.

2D face recognition models are vulnerable to lighting and pose variations between registration and authentication. And while 3D face models are theoretically immune to these issues, they do not appear to offer any advantage in dealing with variation in facial expressions. Instead, many experiments have shown that fusing 2D and 3D techniques for face model creation is more accurate.

Face authentication

Face Authentication is next step, and can only happen when the system has registered and stored a face-print. Face authentication is a 6-step process (Shown in Figure 2).

Steps 1 through 4 are the same in registration process. In step 5, "matching" refers to the system computing the distance between the captured face and the registered face. A match score is awarded based on this computation. Then, in step 6, the system uses that score to communicate whether the authentication is successful or not.

How 3D and 2D face models impact liveness detection

Liveness detection is crucial for maintaining the efficacy of face-based biometric systems. There are many sophisticated spoofing tools—stolen face photos and recorded video; 3D face models capable of blinking, lip movement and other facial expressions; models made of material very similar to human skin. These tools are not difficult to obtain and can be used to fool face-based biometric systems. Hence, anti-spoofing mechanisms are integrated into biometric systems, and used as prime differentiators in the products/solutions space. There are three main indicators used for liveness detection: motion, texture, and life sign.

Motion analysis

The movement of a planer object is significantly different from a 3D object. Motion analysis uses this principle to distinguish between a 2D photo of a face and a 3D face. From the video sequences system determines optical flow for conducting motion analysis. Hence video capture becomes a requirement. Because it is difficult for the system to perform this analysis when motion is not prominent, 3D sculptures can be used to spoof this approach.

Texture analysis

The texture of a real face is different from the texture of an image of a face printed on paper. Texture analysis uses this difference to detect fraud. The analysis looks for print failure and image blur to differentiate between a real face and a photo. In order to effectivity differentiate, the system must be able to recognize different paper and printing textures. Texture analysis can be made ineffective if someone uses a photo displayed on a screen, because a screen will produce very little texture information. In such low-texture scenarios, motion analysis can be combined for a better result.

Life sign detection

Life sign detection can be carried out in two ways, based on either active and passive user participation. In the first case, the user is subjected to a motion challenge. Once the user performs the motion challenge, the system compares facial model values with an ideal threshold value, and uses this comparison to determine liveness. The second approach looks for signs of life through movements like blinking eyes to determine liveness. A system capable of doing life sign detection becomes almost immune to spoofing by 2D face images and static 3D sculptures, but a 3D sculpture with fake liveness action can be used to fool the system. Life sign detection does not rely on textures, although it may need user collaboration and mainly depends on face parts detection.

3D near-infrared cameras in mobile

One of the more accurate ways of creating 3D face models is with an invisible near-infrared (NIR) camera, which eliminates the dependency on ambient light. The NIR-based facial recognition system works by casting tiny dots on a person's face. The camera then captures the reflections off those dots, using alternation of reflected pattern and/or time of return to create a 3D image of the person's face.

The latest smart phones are equipped with NIR-based cameras in the front to allow users to unlock their phones with facial recognition. Face-based biometric authenticator services companies are in the process of getting low-level API so that they can seize the opportunity to provide NIR-enabled 3D facial biometric authentication services in phones. API specifications for manufacturers may vary, making the job of the biometric service provider more complex. EMVCo and the FIDO Alliance have joined hands and are expected to come out with new specification standards for mobile wallet providers and payment application developers to support Consumer Device Cardholder Verification Method (CDCVM). Hopefully, increasing adaptation of FIDO standard will standardize and simplify this ecosystem. Another anticipated benefit of this new specification is additional risk management, leading to a reduction in the number of times a consumer needs to authenticate their face in order to approve payment within the given period.

Considerations for biometrics implementation

The field of computer vision pertaining to face biometrics is moving at a very high speed, and innovations are surfacing that promise greater accuracy in face identification and authentication. With so much in flux, knowing how to choose the right solution for a given situation is critical. The following considerations can help.

The right use case

The proper business case is a basic prerequisite for any successful implementation. One needs to understand the broader picture and consider the questions in Figure 3 before making a final decision about the face-based customer identification and authentication solution.

Answering these questions encourages a holistic point of view, and helps keep implementation on track while preparing for extensions in the future.

Standards and guidelines

There are at least five categories of standards and guidelines that we need to be aware of when choosing a solution in this space: ISO, FIDO, independent third-party testing, applicable country-specific guidelines, and applicable company policy. From an implementation

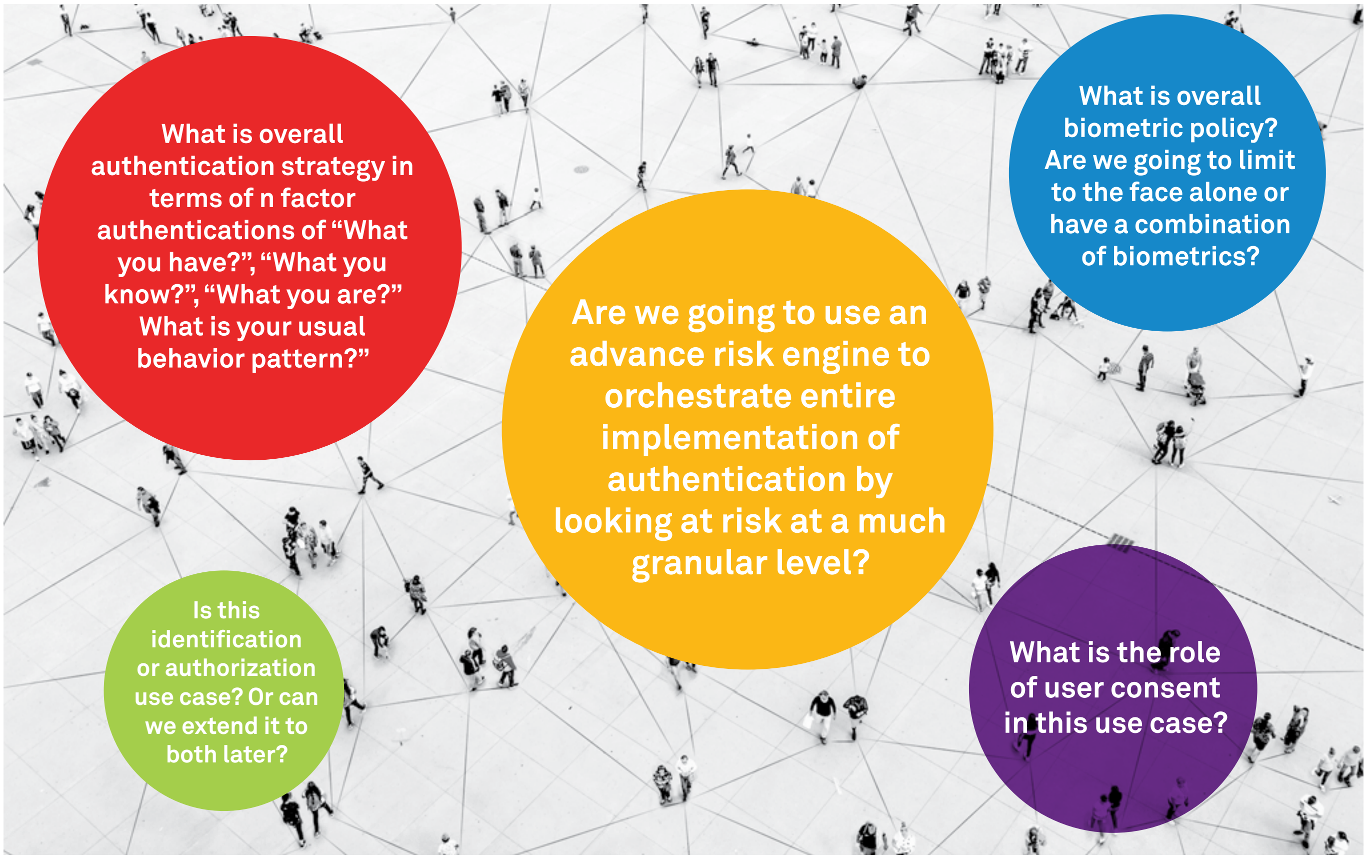
What is overall authentication strategy in terms of n factor authentications of "What you have?", "What you know?", "What you are?" What is your usual behavior pattern?"
What is overall biometric policy? Are we going to limit to the face alone or have a combination of biometrics?
Are we going to use an advance risk engine to orchestrate entire implementation of authentication by looking at risk at a much granular level?
Is this identification or authorization use case? Or can we extend it to both later?
What is the role of user consent in this use case?

Figure 3: Questions to consider when choosing face-based customer identification and authentication solutions.

Biometric Definitions	What it is?	Performance level as per FIDO Alliance
False Accept Rate (FAR)	The proportion of verification transactions with wrongful claims of identity that are incorrectlyconfirmed.	Shall meet the requirement of less than 1:10,000 for the upper bound of 80% confidence interval. FAR is measured at the transaction level.
False Reject Rate (FRR)	The proportion of verification transactions with truthful claims of identity that are incorrectly denied.	Shall meet the requirement of less than 3:100 for the upper bound of 80% confidence interval. FRR is measured at the transaction level.
Impostor Attack Presentation Match Rate (IAPMR)	Proportion of presentation attacks in which the target reference is matched.	The evaluation measures the Impostor Attack Presentation Match Rate for each presentation attack type, as defined in ISO 30107 Part 3.

Figure 4: Biometric definitions for acceptance.

perspective, a well-rounded view of applicable standard guidelines are critical. Here, we focus on one of the critical elements of specification: the biometric definitions for acceptance as shown in Figure 4.

The FIDO alliance provides comprehensive assistance to certify biometric components or the entire sub-system. Their Authenticator Certification Levels are an example of this, providing a framework for security requirements and testing. Independent third-party testing is the best way to confirm such performance levels, because it harnesses the knowledge of experts in this area.

Closing note

We are experiencing significant technological advancements in the biometric area. The ability to identify and authenticate a digital subject will no longer be a challenge. However, the business use cases for this technology will remain a crucial ethical question, especially if the technology for facial recognition is misused, disregarding personal privacy.

A parallel track of research is currently looking to counter such misuse and to protect privacy. Solutions like lens-shaped masks, face projectors, goggles fitted with LEDs, CV dazzle makeup, and headscarves decorated with faces are being explored as means to prevent facial recognition from identifying a face correctly. Investments in technology research for biometric identification and authentication need to be balanced by adequate effort to reach a widespread consensus about use of this technology. There needs to be open debate about global policy and standards governing use of biometrics.

References

1. “An overview of face liveness detection” from International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014 by Saptarshi Chakraborty and Dhrubajyoti Das
2. FingerTec whitepaper on Face Recognition Technology
3. https://fidoalliance.org – Various reference are fido alliance site
4. “What is a Presentation Attack? And how do we detect it?” by Christoph Busch et. al
5. Consumer Biometrics Market & Technologies Trends 2018 report by Yole Development http://www.yole.fr/iso_upload/News/2018/ PR_BIOMETRICS_CONSUMER_IndustryOverview_YOLE_Dec2018.pdf
6. Face Image Quality Evaluation for ISO/IEC Standards 19794-5 and 29794-5 by Jitao Sang, Zhen Lei, and Stan Z. Li
7. Facing the Future: New Applications and Trends in Facial Recognition — a blog by Anne Corning
8. FIDO, EMVCo Prep for Pay-by-Selfie Era – a new article by Tara Seals in infosecurity magazine
9. “How Facial Recognition Systems Work” by Kevin Bonsor & Ryan Johnson
10. Comparison of 2D/3D Features and Their Adaptive Score Level Fusion for 3D Face Recognition – a whitepaper by Wael Ben Soltana, Di Huang, Mohsen Ardabilian, Liming Chen
11. Multi-Modal 2D and 3D Biometrics for Face Recognition a whitepaper by Kyong I. Chang KevinW. Bowyer Patrick J. Flynn
12. Source: Consumer Biometrics Market & Technologies Trends report, Yole Développement, 2018 - https://www.slideshare.net/Yole_
13. Developpement/consumer-biometrics-market-and-technologies-trends-2018-yole-dveloppement

About the Author

Santanu Dutta

Innovation Engineering Leader for Banking and Financial Services, Wipro

Santanu has 23 years of industry, domain and technology experience in software product and solutions. He is leading an initiative christened as “miliu” – Wipro’s concept bank of future. This initiative conceptualizes the art of possible for a future digital bank and develops innovation accelerators synergizing IPs/solutions of Wipro and its partners.

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035,India
Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 175,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,please write to us at
info@wipro.com