White Paper

Four Key Trends Shaping Mobile & Wearable Biometrics
CONTENTS

Multimodal Mobile Biometrics........................................................................................................3
Biometric Innovation .........................................................................................................................4
Consumer Choice .............................................................................................................................5
Liveness and Spoof Detection ...........................................................................................................6
It is six years since Goode Intelligence first covered mobile biometrics and in that time biometric authentication on smart mobile devices has become commonplace. This white paper from cybersecurity analysis and consulting company Goode Intelligence (GI) identifies four trends currently shaping mobile biometrics:

1. Multimodal biometrics
2. Biometric Innovation
3. Consumer Choice
4. Liveness and Spoof Detection

Over the six years since Goode Intelligence first covered this market in 2011 it has grown significantly year-on-year with mobile biometric authentication becoming common place in a number of applications, in particular to secure financial services.

The market is still evolving with a number of different models that developers and service providers can adopt to provide convenient friction-free user authentication. It is part of the wider “password replacement” movement that includes other two-factor (2FA) and multi-factor authentication technologies. Password and knowledge-based user authentication mechanisms still dominate but with many of the largest digital providers moving to offer 2FA and two-step verification (2SV) services the time is right for a new era of convenient user authentication. SMS-based 2SV dominates the consumer 2FA market but there are signs with rising adoption levels that the additional costs of terminating SMS Application to Person (A2P) 2FA messages and the friction it adds to the authentication experience is creating opportunity for mobile biometric authentication solutions; especially with the rise and variety of device-based biometric authentication services.

Mobile Biometric Authentication offers significant advantages versus other MFA technology especially code based technologies where a user has to read and enter in a one-time-password (OTP) delivered by SMS – a messaging technology that was never intended to be used for security and has been deprecated by the US governments technology standards authority, NIST.\(^1\)

The opportunity for consumer mobile biometric authentication is vast – use of Mobile Two-Factor Authentication (M2FA) is increasing with the availability of simple SMS based two-step verification (2SV) services but Goode Intelligence calculates that only six percent of the addressable market is adopting stronger authentication currently.

\(^1\) https://pages.nist.gov/800-63-3/sp800-63b.html
Four Trends Shaping Mobile & Wearable Biometrics

In the third edition of our influential analyst report, "Mobile & Wearable Biometric Authentication – Market Analysis & Forecasts 2017-2022", we identify four major trends currently shaping mobile biometrics.

1. Multimodal Mobile Biometrics
2. Biometric Innovation
3. Consumer Choice
4. Liveness and Spoof Detection

MULTIMODAL MOBILE BIOMETRICS

Up until very recently biometric sensors have been integrated into mobile and wearable devices as a single modality, e.g. a single sensor is used by its user for authentication. This situation is changing.

During 2016 and into 2017 there is a growing trend for multimodal biometric authentication where multiple biometric sensors and applications are available on smart mobile devices. They can be used in conjunction with one other, for instance voice and face to improve security, or singularly to match the security risk and context for its use, for instance voice in a less crowded area or face when the light conditions are favourable.

This is being led by both biometric sensor manufacturers in delivering packaged multimodal biometric solutions to their OEM customers and with developers and service providers by integrating software biometric applications into their mobile apps; often supplied by their authentication partners – for instance RSA's Adaptive Authentication mobile SDK that supports native fingerprint and EyeVerify’s Eyeprint ID.

Activity from the fingerprint sensor manufacturers has accelerated in the first half of 2017 with Synaptics announcing in January 2017 a partnership with facial recognition specialist, Key Lemon, in developing a multimodal solution combining fingerprint and face. Synaptics are calling this their "multi-factor biometric fusion engine" and they anticipate adding other biometric modalities at a later date.

Fingerprint Cards (FPC) have also entered into the multimodal biometric authentication market with the acquisition of iris recognition specialist, Delta ID – announced on 1st February 2017 and finalized on 7th June 2017.

Mobile OEMs are beginning to support this trend with Samsung launching their latest Galaxy Smartphone 8 and 8+ on 29 March 2017 supporting three separate biometric modalities; Fingerprint, Iris and Face. To support a large, bezel-free, display Samsung has located the fingerprint sensor on the rear of the device next to the camera.

The integration of multiple biometric technologies by mobile device OEMs will be a key feature of the market during the period from 2017 to 2022. Fingerprint will co-exist with other biometric modalities (both hardware sensor and software app) including iris, face, voice and eye-vein. These will either be available as part of the OEM integration, as with the Samsung Galaxy S8 supporting fingerprint, face and iris out of the box, or via mobile apps – either stand-alone or more likely integrated into an app through use of a biometric SDK.
BIOMETRIC INNOVATION

Innovation in biometric technology is responding to a combination of factors including:

- industrial design needs from the mobile OEMs;
- consumer feedback; and
- Service provider requirements.

Mobile OEMs are bringing to market larger active touchscreen smart mobile devices with little or no bezel and without physical buttons. This is driving biometric sensor manufacturers, in particular fingerprint sensor providers, to investigate solutions that can be integrated into these devices. For fingerprint sensors, there are technical issues in getting user experience and performance right. Samsung has had to locate its fingerprint sensor on the back of the device and there are rumours that Apple may delay the launch of the iPhone 8 to ensure that the experience and performance of the under-glass sensor is right. This is also creating opportunity for non-capacitive sensor technology including optical and ultrasound.

Optical and ultrasound sensors can also assist in improving liveness and spoof detection as they can capture blood vessel characteristics and even read a person’s pulse.

For other modalities, there is the emergence of specialist camera hardware that can support Iris and 3D facial recognition. GI believes that these modalities will work in conjunction with fingerprint biometrics, offering a different user experience that will be suitable for a range of applications. Another modality that could be suitable for mobile and is already being used on wearable devices is ECG (heart) – this modality has great opportunity in deterring spoof attacks as a live ECG is difficult to copy.

MOBILE FINGERPRINT TOP TRENDS

Eight top trends for fingerprint biometrics on smart mobile devices

1. UNDER-GLASS
   - A trend for smart mobile design is to remove non-active parts of the screen, including bezel and physical start button. A design option is to place the fingerprint sensor underneath the screen glass and not to rely on integration underneath a physical button.

2. SPOOF & LIVENESS DETECTION
   - Spoof and liveness detection solutions enable use of fingerprint for higher value applications. This can be hardware or software based.

3. OPTICAL SENSORS
   - Optical fingerprint sensors are now available for mobile integration and they can provide improved liveness detection and offer under-glass design options.

4. ULTRASOUND SENSORS
   - Ultrasound fingerprint sensors are able to capture 3D fingerprint images and can be located in a variety of physical areas of a smart mobile device, including under-glass and embedded in the case.

5. GESTURE CONTROL
   - Mobile OEMs can leverage their investment in fingerprint sensors by supporting other, non-identity, applications. Supporting gesture control for the sensor can enhance user experience.

6. FLEXIBLE SENSORS
   - One for the future, flexible and foldable devices require flexible fingerprint sensors. Offers potential for non-smartphone devices including IoT and Auto.

7. BIOMETRIC APIs
   - Biometric APIs on the most commonly used mobile platforms, Apple iOS and Google Android, enable third-party access to built-in biometric and security systems.

8. INCREASED PENETRATION
   - Integrated fingerprint sensors on smart mobile devices are no longer solely for flagship models. They are now available for mid and even low-end smartphones for as little as $19.90.

Information drawn from the Goode Intelligence analyst report "Mobile & Wearable Biometrics: Adoption, Market Analysis & Forecasts 2017-2022"
CONSUMER CHOICE

User experience is key in designing any mobile application. Security and identity applications are not immune in having to be convenient and easy to use. As well as consumer choice, it is imperative to match the right biometric modality to each application and user experience requirement. This can be achieved by giving consumers choice in what biometric technology is available to them on a mobile device.

A number of recent surveys have identified that consumers want choice in terms of the biometric technology that is available to them on their mobiles and within their mobile apps. Samsung is enabling choice for consumers in what biometric technology to use to reflect different security requirements and circumstances. The latest Samsung Galaxy S8 smartphone combines fingerprint, face and iris out of the box. With the fingerprint sensor on the rear of the device, a user could use the face unlock feature whilst the device is laying on a surface allowing the user to not have to pick the mobile up to unlock using the rear-positioned fingerprint sensor. Iris can provide a higher level of security than face and finger so could be used for higher security scenarios including enterprise applications. Consumer choice and distinction between competitors in an ever-crowded marker are key decision makers for device OEMs.

Consumer choice is also being provided by biometric software solutions, either run as stand-alone apps or integrated into an app by use of a biometric SDK. There are an ever-increasing amount of innovative biometric software applications that are being deployed in larger numbers. Table 1 details some of the technology vendors that are active in developing biometric applications and software services – all of these vendors and solutions are covered in detail in the report; Goode Intelligence Mobile & Wearable Biometric Authentication – Market Analysis & Forecasts 2017-2022.

Table 1: Mobile Biometric Applications and Software Services

<table>
<thead>
<tr>
<th>Company / Biometric Application</th>
<th>Biometric Modality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applied Recognition Ver-ID</td>
<td>Face</td>
</tr>
<tr>
<td>BehavioSec</td>
<td>Behavioral</td>
</tr>
<tr>
<td>BioCatch</td>
<td>Behavioral</td>
</tr>
<tr>
<td>EyeVerify Eyeprint ID</td>
<td>Eye-vein</td>
</tr>
<tr>
<td>iProov</td>
<td>Face</td>
</tr>
<tr>
<td>KeyLemon Oasis Face</td>
<td>Face</td>
</tr>
<tr>
<td>Nuance Communications</td>
<td>Voice</td>
</tr>
<tr>
<td>Veridium 4 Fingers TouchlessID</td>
<td>Touchless Fingerprint</td>
</tr>
<tr>
<td>VoiceTrust</td>
<td>Voice</td>
</tr>
<tr>
<td>VoiceVault</td>
<td>Voice</td>
</tr>
</tbody>
</table>
LIVENESS AND SPOOF DETECTION

According to many industry insiders there is a current “arms race” to deliver superior spoof and liveness detection capabilities on smart mobile devices. This is predominantly for fingerprint biometrics as this is the dominant modality but is also extremely relevant for other modalities. With the rise of mobile fingerprint technology and the increasing use of these systems for higher value applications such as payments and banking, there has been an increase in attacks whereby a fingerprint sensor is spoofed. Spoofing involves fooling the sensor and biometric system that the enrolled, authorised, finger has been presented and then performs the necessary action – unlock the device or authorise a payment.

Fingerprint sensor manufacturers and their partners are investing heavily in deploying technology that improves the ability for a sensor to detect fake and spoof attempts and this will be a prime differentiator for 2017.

**Synaptics** announced in February 2016 that it had added anti-spoofing to its SentryPoint biometric fingerprint security suite using proprietary anti-spoofing algorithms to discriminate between spoof and actual fingers.

In October 2016, ZTE became the first mobile OEM to integrate **Goodix’s ‘Live Finger Detection’ (LFD)** technology into the Axon7 Max smart mobile device. The sensor combines a standard fingerprint sensor with an optical fingerprint sensor that emits infrared light. That means it can scan the underlying tissue of a fingerprint, which should go a long way in preventing spoofing. The sensor is also able to detect a user’s pulse, offering fitness tracking applications.

The current dominant fingerprint sensor supplier for Android devices, **Fingerprint Cards**, also released an anti-spoofing solution called **FPCLiveTouch** in February 2016.

Spoof and liveness detection services are also available as part of fingerprint matching software; Precise Biometrics’ acquisition of anti-spoof and liveness detection specialists, NexI.D, has enabled support within the popular **Precise Biometric BioMatch Mobile** solution.

Goode Intelligence believes that the capability to detect live fingers and to deter spoofing attacks will be a prime consideration for mobile OEMs deploying the next generation of fingerprint sensors in smart mobile devices and will enable a new generation of fingerprint biometric authentication use cases and applications.
Mobile & Wearable Biometric Authentication Market Analysis and Forecasts 2017-2022 is a 175 page analyst report that provides an investigation into the use of biometrics for authentication on smart mobile and wearable devices.

The report includes analysis of the main drivers and potential barriers for deployment, adoption case studies, interviews and six-year market forecasts for the years 2017-2022.

About Goode Intelligence
Since being founded by Alan Goode in 2007, Goode Intelligence has built up a strong reputation for providing quality research and consulting services in cyber security including:

- Biometrics
- Mobile and IoT Security
- Financial Services / Fintech Security
- Authentication and Identity
- Internet of Things Security
- Regtech and Compliance

For more information on this or any other research please visit our [website](http://www.goodeintelligence.com).

Facts & Figures
The market for mobile biometric authentication offers considerable opportunities for those involved in developing technology for it with a forecast of revenue CAGR of over 12 percent for the six year period 2017-2022. The market will grow from $3.189 billion in 2017 to $6.265 billion in 2022 – both hardware and software biometric solutions.

Greater availability of smart mobile devices with integrated biometric technologies and the ease-of-integration for biometric software technologies will ensure that over 3.3 billion users will be benefiting from secure convenient biometric authentication by 2022.