3 STEPS TO PREPARE FOR MULTIMODAL BIOMETRIC PAYMENTS

Whitepaper

JUNIPER RESEARCH

1.1 Introduction

With password-based solutions becoming increasingly impractical, service providers have begun implementing an alternative second factor; ‘something I am’, using a fingerprint, iris, facial feature or vein pattern to establish an individual’s identity.

Biometric identifiers afford the user an additional layer of handset security. There is increased reliance on biometric user identification in the security industry itself; iris and fingerprint scanning is commonplace in the US, as well as Europe and some new world countries including Australia. In the mobile arena, biometric recognition technologies are increasingly being deployed to identify handset owners and to allow them to unlock their handsets, as well as being used as a method to authenticate the user when making a payment through mobile devices.

1.2 Key Biometrics Trends

1.2.1 Biometrics Need to be Ready for Basic Hardware

Although biometrics is currently associated primarily with flagship mobile devices, several modalities are being developed that utilise more basic hardware. From voice recognition simply needing a microphone to facial and eye biometrics just needing a camera, many biometrics providers need to be prepared to build biometrics for the most basic of smartphone requirements.

The ability to deploy these continuous biometrics, as well as the use of commodity hardware in several biometric modalities mean that biometrics-as-a-service is emerging. Companies can supply biometric APIs to apps that need biometric authentication as part of their security, without requiring specialised hardware.

This means that, with the use of cloud-based AI (Artificial Intelligence) as the driving force for many of these companies, such offerings will be attached primarily to HCE-based payments, where it is a payment service. This is because both authentication and payment assume the same connection to the cloud, so can take advantage of higher levels of processing power to run the required authentication checks.

1.2.2 Biometrics-as-a-Service is Here

With several biometric modalities relying on increasingly common components in smartphones, from the increasing prevalence of fingerprint sensors to the ability to track and cross-reference smartphone behavioural data, several companies are offering platforms which provide biometrics-as-a-service or identity-as-a-service. This is because of the increasing prevalence of standard hardware, such as ARM’s TrustZone, across many devices. With ARM providing the vast majority of chip designs for Android phones, and Apple supplying iOS, the hardware requirements for biometric storage and authentication are becoming much more standardised.

That being the case, producing cloud-based platforms which can use biometric identifiers as security options has become far easier. These players have multimodal biometric authentication, as well as some behavioural verification, as the next steps in their offering. This is because, as a cloud-based service, the ability of the device to compute

the machine learning capabilities becomes moot; all that is needed is for the software to relay detected inputs (whatever they may be) to the cloud, where the processing and verification can take place. With a device that is always connected to the Internet, this can even take place on a continual basis.

As a result, Juniper believes biometrics-as-a-service is where true multimodal biometrics will have their biggest impact. As behavioural verification data can be passively collected, there are no additional barriers to convenience compared to conventional authentication.

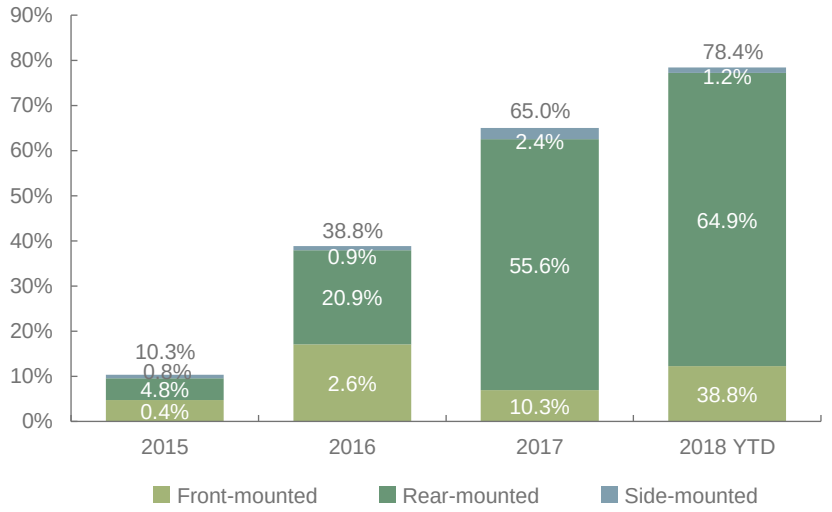
1.2.3 Which Modalities?

There are an increasing range of biometric modalities, which have a wide variety of hardware requirements. These will limit the possibilities of what can be done with each modality to a degree, putting the onus on software providers to come up with algorithms that can produce more and more exacting information from basic hardware. Facial recognition is a key case here. Face ID, Windows Hello and RealSense all utilise multiple cameras and, in some cases, blends of infra-red and traditional cameras, not all smartphones have this capability. This is particularly problematic given that most smartphones with third party biometrics providers are Android devices. The wide range of Android OEMs means that to reach a broad base of users, biometric security providers have to be ready to use basic hardware as part of their biometric authentication process.

i. Fingerprint Biometrics

Fingerprint biometrics are becoming increasingly expected. The number of smartphone models including fingerprint sensors is now increasing sharply. While data from GSMarena.com suggested that only 3% of smartphone models launched in 2014 featured fingerprint sensors, by 2017 this had risen sharply to 65%, and to date nearly 80% of smartphones announced or released in 2018 have fingerprint sensors (see figure 1). However, these are potentially some of the most limited by hardware, needing a discrete sensor where others will use a multi-purpose device like a camera or microphone.

Figure 1: Proportion of Released Smartphones with Fingerprint Sensors, 2015-2018 YTD (%)



Source: Juniper Research, GSMArena

ii. Voice Biometrics

With the rise of voice assistants, voice is becoming increasingly popular as a transaction method, but currently the consumer-grade solutions are

not advanced enough in their voice recognition technology to allow that to stand on its own as a method of authentication.

In theory, voice could provide this, given the prevalence of voice assistants in IoT (the Internet of Things). However, current security levels for voice commerce are relatively low. This means that to have a fully secure IoT payments system, a more advanced voice biometrics solution is required, with more precise voice identification algorithms, like those currently used by banks for voice authentication over the phone.

iii. Facial Recognition

While payment biometrics have for several years now been focused on fingerprints, there have been multiple initiatives from a wide range of stakeholders to replace it with facial recognition. Initiatives have included Google's Hands Free payment service and, more relevant to the mobile space, Apple's Face ID and Mastercard's Selfie Pay.

Figure 2: Smartphone Notch Designs

Note: from top, left to right: iPhone X, The Essential Phone, Huawei P20, OnePlus 6, Xiaomi Mi 8, LG G7

Source: Courtesy of Apple, Essential, Huawei, OnePlus, Xiaomi and LG

In addition, facial recognition places less constraints on smartphone design, such as the ability to use fully glass body or bezel-less designs, both of which are hard to implement with biometrics that require dedicated sensors. These would still need to have some surface area to allow a selfie camera, but this only constrains one portion of the smartphone display, and 'notches' have already become a common feature in flagship smartphone design, following the iPhone X release (see figure 2 above).

iv. Multi-modal & Behavioural Biometrics

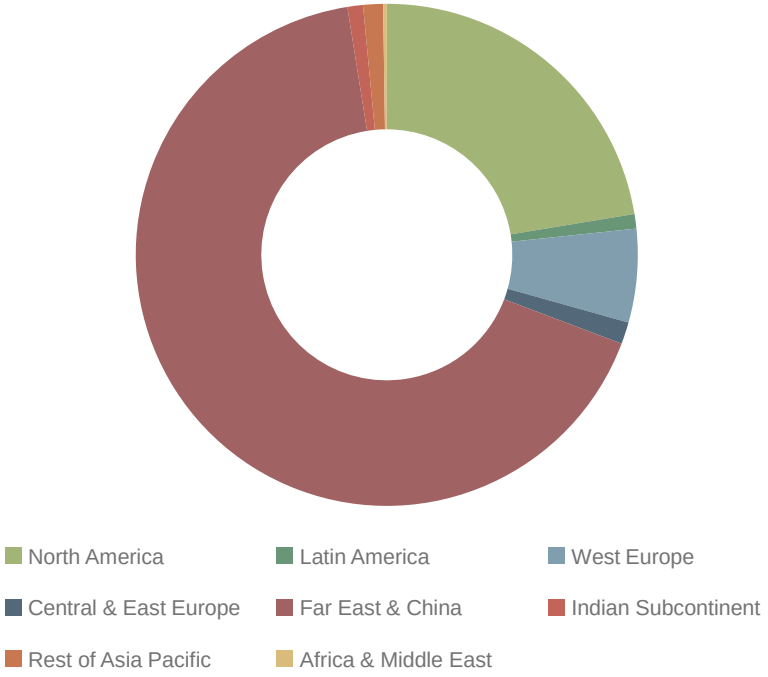
What began with fingerprint sensors being integrated into smartphones has now emerged as a full suite of biometric modalities. Some mobile vendors can now offer multiple forms of biometric modalities, which is driving security software companies to provide multimodal solutions.

The degree of device sensors now present in smartphones allows a degree of positional and usage tracking which differentiates one user from another. These behavioural signifiers can be read by software that is installed on a device or connected through the cloud, meaning the individual behaviour of a user can be tracked. Several companies are now moving to this behavioural biometric model to provide a level of continuous authentication, in addition to single-time authentication when required.

1.3 Biometrics Forecast Summary

The value of all smartphone biometrically authenticated transactions is expected to increasese from $123.5 billion in 2018 to over $2 trillion in 2023, an average annual increase of 76.1%.

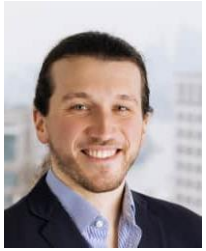
Figure 3: Value of Biometrically-Authenticated Sales in 2023 (m), Split by 8 Key Regions: $2 trillion



Source: Juniper Research

- In terms of overall value, the China and the US are the 2 largest markets, with China being the clear leader with over $1.2 trillion transacted via biometrics in 2023, 42.3% of the global market value. However, with the landscape dominated by local players, the more international market may be the only option unless China's market fragments, which is unlikely in the near future.
- With an increasingly mobile-based POS system and a growing number of smartphone users, Latin America is the fastest-growing region for biometric authentication, with a CAGR of over 180% throughout the forecast period.
- For most emerging economies, there will be an overall decline in average transaction values over the forecast period, as the technologies reach new users who have limited purchasing power, driving the average transaction value down.
- We expect some countries in West Europe to provide some of the highest transaction values throughout the forecast period, with most Nordic countries and Germany remaining above $50 per transaction over the next 5 years.

1.4 Mobile Biometrics Movers & Shakers



Alesis Novik

AimBrain

CTO & Co-Founder

Alesis Novik is the CTO and co-founder of AimBrain. With the vision to provide the market with a smart and transparent biometric experience, He has helped to guide AimBrain to its unique position as the world's only multi-module, biometric security solution.

Novik holds degrees from Vilnius University and the University of Edinburgh. During the course of his academic career, he participated in Google's Summer of Code Program. More recently, Novik has spent time at CERN and at Level E Capital. He has also completed 3 years of PhD work.

Gino M Pereira

NXT-ID

CEO & Co-Founder

Gino Pereira has been NXT-ID's CEO since its inception. He has over 30 years of executive, operational and financial experience with technology companies in the US, Europe and the Far East. He has also helped to develop several technology start-ups, as well as served in an executive capacity in a large multinational public company.

Pereira was CFO, then CEO of Technest Holdings, a publicly quoted defence contracting company, from 2004 to 2011.

He is a Fellow of the Chartered Association of Certified Accountants (UK) and has an MBA, with a specialty in finance, from the Manchester Business School in the UK.

Vlad Sejnoha

Nuance

CTO

As Nuance's CTO, Vlad Sejnoha oversees Nuance's research and focuses on core technology and product strategy, with an emphasis on emerging areas including natural language processing and mobile applications.

Prior to joining Nuance, Sejnoha was the Chief Scientist at L&H and earlier at Kurzweil AI. There he was responsible for creating technology for a number of commercially successful speech recognition products, including large vocabulary continuous speech dictation systems.

Sejnoha has over 20 years' experience in the field of speech recognition and has 13 US patents. He earned a BSc and Master's degree in Electrical Engineering from McGill university.

Carsten Ahrens

G+D Mobile Security

CEO

Carsten Ahrens is the CEO of Giesecke+Devrient Mobile Security GmbH. As well as his duties as CEO, he is responsible for the areas of Strategy, Compliance, Sales, Divisions, Marketing and Communications, and the Technology Office. Moreover, he is currently temporarily in charge of Research and Development, Personnel, Operations, and Professional Services.

Ahrens has been working in the Mobile Security unit at G+D since 2013, initially as the Manager of the Telecommunication Industries division and later as the Chief Sales and Marketing Officer.

He held various management positions before joining G+D, including CTO/COO at Funkwerk AG and Managing Director at Ericsson GmbH.

Edward Casey

IDEMIA

CEO of North America Identity & Security Business Unit

Ed Casey was appointed as CEO of IDEMIA's North America Identity & Security Business Unit in January 2018, as part of an executive reshuffle to further operational integration in the company.

Before joining IDEMIA, Casey spent 13 years in Serco Group. He held various senior management positions at Serco, including Group COO and Member of the Board of Directors, Acting Group CEO, and CEO of Serco's Americas Division. Under Casey's leadership, the Americas business tripled in size and successfully integrated 2 acquisitions: RCI and SI International.

Prior to Serco, Casey held senior management positions in the energy, investment banking and private equity fields at NP Energy, an energy marketing business he founded and later sold; Tenneco Energy; LG&E Energy; The Blackstone Group; and Fremont Group.

Toby Rush

ZOLOZ

CEO & Founder

Toby Rush founded EyeVerify in January 2012 and was its CEO. Rush is the founder of TotalTrax (also known as, Rush Tracking Systems), and was CEO and President since February 2003 to December 2011. He was Product Manager and then Vice President of Product Development for SAT Corporation.

Rush has achieved national recognition as an expert on mobile and wireless technologies. He began his career with Accenture, implementing large systems such as SAP and PeopleSoft. He was Senior Consultant & Project Manager at BSI Consulting from May 1999 to January 2002. He was also Analyst at Accenture from May 1998 to May 1999.

Rush has a BSc Engineering in Mechanical Engineering from Kansas State University.

Order the Full Research

Juniper's **Mobile Payment Security** research offers the most in-depth assessment to date of the opportunities and challenges across the payment tokenisation and biometric authentication sectors. Through essential industry forecasts and interviews with leading players, it assesses the impact of a range of recent legislation and industry initiatives on the security space. Additionally, it is the only research available providing data and forecasts for payments split by biometric type.

Key Features

- **Sector Dynamics**: Analysis of key market developments and primary challenges across the payment security space.
- **Leading Industry Forecasts:** Provided for the size and growth of tokenisation, biometric POS payments and remote payments, including Fingerprints, Facial Recognition, Iris Scanning and Voice Biometrics.
- **Juniper Leaderboards:** Provided for the tokenisation and biometrics industries, with attendant heatmap based scoring of 21 key players.
- **Interviews**: With leading players across the mobile payments and security value chain, including Acuant, AimBrain, First Data Corporation, Gemalto, Giesecke+Devrient, IDEMIA, Nuance, NXT-ID, Precise Biometrics, Rambus, Stripe.

What's in this Research?

1. **Executive Summary & Core Findings** – Top-level report summarising key trends, competitive analysis and market forecasts, allied to a series of key takeaways and strategic recommendations for C-level executives. (PDF)
2. **Deep Dive Strategy & Competition** – Strategic analysis of market dynamics, drivers and trends affecting the biometrics and tokenisation spaces, together with capability assessment and vendor Leaderboards for each sector. (PDF)
3. **Deep Dive Data & Forecasting** – Market sizing and analysis by region and sector, together with 5 year forecasts for key metrics, including biometric devices, users, tokenised transaction volumes, biometric transaction volumes and value. (PDF)
4. **Interactive Forecast Excel** – Highly granular dataset nearly 10,000 datapoints, allied to an Interactive Scenario Tool giving users the ability to manipulate Juniper's data. (Interactive XL)

Publications Details

Publication Date: March 2018

Author: James Moar

Contact Jon King, Sales & Marketing Manager, for more information:
Jon.King@juniperresearch.com

Juniper Research Ltd, Church Cottage House, Church Square, Basingstoke, Hampshire RG21 7QW UK

Tel: UK: +44 (0)1256 830002/475656 USA: +1 408 716 5483 (International answering service)

http://www.juniperresearch.com