National and Civil ID White Paper

This study examines the numerous electronic credentials and processes emerging within the National and Civil ID market.

Rawlson O`Neil King
Lead Researcher, Biometrics Research Group, Inc.

Money 20/20

NOVEMBER 2-6, 2014
ARIA, LAS VEGAS

Security, Identification and Validation are the keys to creating new frictionless commerce experiences. With a discussion centering on technologies like Biometrics, Tokenization, Predictive Analytics and Big Data, Money20/20 brings together innovators helping define the industry.

One Unprecedented Event

6,500+ attendees, including 500+ CEOs,

from 2,000+ companies and 50+ countries

You don't want to miss the **Event of the Year**. Money20/20 will be held November 2-6, 2014 at the Aria Resort & Casino in Las Vegas. Join the global community of leaders convening at Money20/20.

Use code BIOMET20 and **save 20%** off our current registration rate, **courtesy of Biometric Update.**

WWW.MONEY2020.COM • INFO@MONEY2020.COM

TABLE OF CONTENTS

Research Methodology

Biometrics Research Group, Inc. uses a combination of primary and secondary research methodologies to compile the necessary information for its research projections.

The conclusions drawn are based on our best judgment of exhibited trends, the expected direction the industry may follow, and consideration of a host of industry drivers, restraints, and challenges that represent the possibility for such trends to occur over a specific time frame. All supporting analyses and data are provided to the best of ability.

Primary Research

Biometrics Research Group, Inc. conducts interviews with technology providers, clients, and other organizations, as well as stakeholders in each of the technology segments, standards organizations, privacy commissions, and other influential agencies. To provide balance to these interviews, industry thought leaders who track the implementation of the biometric technologies are also interviewed to get their perspective on the issues of market acceptance and future direction of the industry.

Biometrics Research Group, Inc. also applies its own proprietary micro- and macroeconomic modeling using a regression analysis methodology to determine the size of biometric and related-industry marketplaces. Using databases of both publicly and privately-available financial data, Biometrics Research Group works to project market size and market potential, in the context of the global economic marketplace, using proven econometric models.

Secondary Research

Biometrics Research Group, Inc. also draws upon secondary research which includes published sources such as those from government bodies, think tanks, industry associations, internet sources, and Biometrics Research Group, Inc.'s own repository of news items. This information was used to enrich and externalize the primary data. Data sources are cited where applicable.

National and Civil ID

Identity security is a critical concern to governments that have responsibility for national security, revenue protection and law enforcement. False identities underpin some terrorist and criminal activity and undermine border and citizenship controls and efforts to combat terrorist financing and financial crime. Identity theft is also a major invasion of privacy and a serious concern due to legal and financial consequences. In order to combat these security challenges, it is essential to any country's security and economic interests that the identities of persons accessing government or commercial services, benefits, official documents and positions of trust, can be accurately verified.

Biometrics Research Group, Inc. defines "National ID" or "Civil ID" as a general identifier used by governments to verify a citizen and establish a link of trust. National or Civil ID is a means for tracking citizens, permanent residents, and temporary residents for the purposes of work, taxation, government benefits, health care, and other governmentally-related functions. Examples of this could be for the purposes of document issuance, border management, voter registration or employment background checks. Typically, National or Civil ID programs are large-scale identity management solutions.

Biometric Research Group estimates that the total number of unit shipments of National or Civil ID documents worldwide will be at 500 million by the end of 2014 and will reach 1.1 billion by 2018. This number includes national identity cards, e-Passports, e-Health cards, eIDs, drivers' licenses and other electronic documents.

Governments have a vested interest in knowing who is being issued a driver's license or who is receiving state-sponsored health care. Civil or National ID allows governments to track service delivery and consumption in a unified fashion unlike traditional national ID number systems.

National ID number systems vary in implementation worldwide, but in most cases, a citizen is issued an identification number and credential, such as an identification card, at birth or when they reach a legal age -- typically the age of 18. Non-citizens may be issued such numbers when they enter the country, or when granted a temporary or permanent residence permit.

Mandatory nationwide identification systems have also been implemented in a number of countries including Argentina, Belgium, Colombia, Germany, Italy, Peru, and Spain. While these schemes vary by country, individuals are typically assigned an ID number, which is used for a broad range of identification purposes.

Large amounts of personal data such as name, birth date, place of birth, gender, eye color, height, current address, photograph, and other information is linked to these ID numbers and stored in centralized databases. Many countries are now modernizing their ID databases to include biometric identifiers that authenticate or verify identity based on physical characteristics. Biometrics Research Group defines biometrics as measurable physical and behavioral characteristics that enable the establishment and verification of an individual's identity. Biometric patterns can be anything from fingerprints, iris scans, palm prints, gait, facial recognition or even voice recognition.

Use Case: United States

While many countries issue such credential and numbers for a singular purpose, over time, they become a de facto national identification number. For example, the United States developed its nine-digit Social Security number system as a means of disbursing Social Security benefits. However, due to function creep, the number has become used for other purposes to the point where it is almost essential to have one to, among other things, open a bank account, obtain a credit card, or drive a car.

The Social Security number however does not constitute a "true national identity card", since there is no federal agency with nationwide jurisdiction that directly issues such cards to all U.S. citizens for mandatory regular use, or to access a multiplicity of services. In the United States, citizens are first issued a birth cer-

tificate as an initial identification document. Although issued by the individual states, it is the first document establishing U.S. citizenship. After that, citizens are typically issued a Social Security number.

The Social Security number was originally intended to ensure accurate reporting of payroll contributions so that an employee's Social Security benefits could be adjusted accordingly, and then the employee could claim their benefits upon retirement. Because their original purpose was so limited, Social Security cards were not designed with the rigorous security measures normally expected of identity documents. They did not, and still do not, have a photograph of the bearer or a physical description. However, in the absence of a national identity card, the Social Security number has become the de facto national identifier for tax and credit purposes. In turn, the epidemic of identity theft in the U.S. since the 1990s has led to various proposals for a national identity card, which have generally been rejected.

The United States did enact the REAL ID Act of 2005, which sets forth requirements for state driver's licenses and ID cards to be accepted by the federal government for "official purposes", as defined by the Secretary of Homeland Security. The Secretary of Homeland Security has currently defined "official purposes" as presenting state driver's licenses and identification cards for boarding commercially operated airline flights and entering federal buildings and nuclear power plants. The Act also defines how data should be collected and design commonalities that should be incorporated in the card.

The REAL ID Act was implemented as an acknowledgement to the fact that most U.S. citizens use their driver's licenses as their de facto official identification card. In most states, a driver's license must be carried at all times when operating a vehicle, and must be presented to law enforcement officers upon request. Licensing authorities also make photo based identification cards available for those who do not have driver's licenses. The driver's license is also often requested by private businesses to verify identity, especially in combination with the use of a credit card or the purchase of alcoholic beverages or cigarettes. Auto insurance companies usually request driver's license numbers from drivers seeking insurance for their vehicles. The companies have real-time access to driving records and can immediately access a person's record to assess the risk of insuring them.

Although most American adults carry their driver's license at all times when they are outside their homes, there is no legal requirement that they must be carrying their license when not operating a vehicle. The ubiquity of the driver's license makes it the most important piece of ID, followed by the passport.

By law, an unexpired U.S. passport or passport card is conclusive proof of U.S. citizenship and has the same force and effect as proof of United States citizenship as certificates of naturalization or of citizenship, if issued to a U.S. citizen for the full period allowed by law. The passport is a widely issued form of identification since it is unlawful for U.S. citizens to enter or exit the United States without a valid U.S. passport or Western Hemisphere Travel Initiative-compliant passport-replacement document. In 2013, over 13.5 million U.S. passports were issued. The number of U.S. passports issued is expected to rise as increased border security controls are implemented.

International regulations for travelers and immigrants are shaping the National and Civil ID document ecosystem, which include the WHTI and the mandated use of a new generation passport technology in Europe which includes strong encryption and new security features, such as supplemental access control.

ePassport

With countries, including the United States, aiming to replace existing travel documents with electronic passports -- otherwise known as ePassports -- the paradigm has shifted towards a highly secure, truly interoperable international border infrastructure that incorporates fast and reliable identity authentication with biometric verification.

An ePassport is the same as a traditional passport book

with the addition of a small, embedded integrated circuit or chip. The chip stores the same data visually displayed on the data page of the passport, as well as the passport holder's picture stored in digital form. An ePassport also contains a unique chip identification number and a digital signature to detect data alteration and verify signing authority. The document also can store additional data in the chip, as defined by specific issuing governments.

Biometrics Research Group estimates that revenues within the global ePassport market will reach US$10.2 billion by 2015. Vendors that will benefit most from this revenue stream will include:

- Gemalto, an international digital security company providing software applications, secure personal devices such as smart cards and tokens in addition to managed services

- Giesecke & Devrient, a German-based company that provides banknote and securities printing, smart cards, and cash handling systems.

- Morpho, a division of French multinational Safran, which specializes in security solutions; and

- Oberthur Technologies, is another French secure technology company, providing security services in smart cards, printing, identity, and cash protection.

These vendors will work in conjunction with governments around the world to issue the new, standardized and secure travel documents. In our estimation, the emerging ePassport standard will create a higher level of streamlined international border security that can be customized for the specific requirements of each individual country.

Biometric Research Group believes that within the next decade, the ePassport will be the ubiquitous travel document. The research firm estimates that nearly 500 million ePassports have been issued worldwide by over 100 countries and that approximately 485 million are in circulation. Of these, 54 countries have opted to store facial and fingerprint data in the travel document.

eID

In addition to ePassports, governments are embracing the use of electronic credentials. The Biometrics Research Group expects the market for electronic identity (eID) cards to reach US$5.2 billion by 2015. With the globalization of world trade, there has been an expansion in the flow of people and goods. In order to prevent counterfeiting and piracy along with terrorism activities, many governments maintain that more reliable identification and authentication methods are required. Consequently, many countries have been deploying eID cards or actively studying approaches to eID card implementation.

An eID card is typically a government-issued document for online and offline identification. Many countries, including Brazil, France, Indonesia, Poland, Russia, Malaysia and the Philippines, have been issuing electronic identity cards that will replace conventional identity cards. Other countries such as Greece, New Zealand and Rwanda have been actively studying their implementation. Even supranational institutions such as the European Union have long been developing technology and policy frameworks for eID deployment. Once a EU framework is completely standardized and accepted by member states, the Biometrics Research Group expects exponential growth within the eID market, since the Schengen Area is composed of over 700 million people.

The typical electronic identity card has the format of a regular bank card, with printed identity information on the surface, such as personal details and a photograph, as well as an embedded microchip.

An eID is more reliable than paper-based ID because it provides more data security with built-in privacy features. The use of digital signatures make

it harder or even impossible to make a forged ID as the duplicate ones would invalidate existing digital signatures.

A citizen with an eID has the ability to use it for various different services, thus making the card multi-purposed. One of the unique aspects of the eID is its ability to authenticate the holder not only in the real world, but also in the virtual world. eID enables it holders to authenticate themselves securely when using an online service, while protecting their privacy.

Apart from online authentication, eID cards can provide users with the option to sign electronic documents with a digital signature for both government and private transactions. An eID is designed to be a trusted authentication mechanism for citizens and businesses to identify themselves in order to electronically access services from across government. Convenience to both users and the authorities is therefore a major advantage of eID systems.

In theory, an eID can be the only piece of identification that a citizen requires for all interactions with government. The cards can therefore be used for multiple purposes, including as a health insurance card for countries with socialized medicine, a social security card, a driver's license, and for general identification. A further unique feature of an eID system is the ability to provide instant multilingual support through online systems.

eID systems also reduce duplication in terms of the time and effort necessary to issue identification across different government departments for varying services. eID systems also allows authorities to centralize the storage of data about citizens, making information footprints accessible from one credential. This benefit will predictably cause many governments to study, approve and implement the technology within the next decade, allowing the market to reach US$11.2 billion by 2020.

Electronic Voting Enrollment

Ensuring quick and precise voter enrollment and identification are cornerstones of any credible election. Biometric systems are increasingly being deployed in the developing world with the aim to ensure a fair and efficient electoral process.
In rich countries, almost everyone has a reliable form of official identification, and biometric technology has traditionally been employed mainly for security and forensics. However, many developing countries suffer from an identity gap where millions of people lack official forms of identification, including birth certificates, national ID cards, and voter cards, which would allow them to access basic services and rights, such as voting.

Closing this "identification gap" has been increasingly recognized as a major goal of economic and social development in developing countries. Just as mobile phones have allowed poorer countries to leapfrog past landline phone connections, biometrics have the potential to help solve identification woes while bypassing the paper-based systems often found in the so-called developed world.

Such biometric systems can include solutions for voter registration, voting, tallying and identification. Common modalities include fingerprint, palm vein, iris and facial recognition. In theory, by using biometric identifiers, the potential of election fraud is minimized, while the voter identification process is accelerated.

In the vast majority of countries where biometrics have been used in voter registration, the motivation for using biometrics has been to "de-duplicate" an election register. Biometric identification helps prevents multiple registrations and also prevents the registration of disqualified voters. For these reasons, the use of biometrics for voter registration has been a popular option exercised by governments throughout Latin America and increasingly in Africa, as indicated in many BiometricUpdate.com articles.

Electors often register multiple times for multiple reasons. The most nefarious reason is for the purpose of voting several times in the hope of influencing an election result or destabilizing the election process. A more common reason is that many election registration processes have not been designed to easily allow for a change of address, causing many electors to re-register without having their existing record concurrently deleted. A registration system tied to biometric authentication could eliminate this problem, as only a singular registration could be associated with a biometric characteristic.

Any well-designed registration process must be able to eliminate instances of multiple enrollment to curb voter fraud. Emerging democracies and countries with chronic electoral problems recognize this. For this reason, a growing number of African countries have opted to use biometric voter registries including Ghana, Kenya, Sierra Leone, Tanzania and Nigeria. In Asia, the Solomon Islands and the Philippines have also deployed such technology. These countries see the benefit of biometric technology as an effective tool for strengthening democracy through establishing legal identities for all individuals, thus facilitating access to fair elections.

Universal National ID

Implementing a universal Civil or National ID program is one of the largest commitments a government can make. The idea behind universal Civil ID or National ID programs is to officially combine different government service functions into one, universal, nationwide identification system.

The most famous example of an all-encompassing Civil or National ID program is India's Universal ID program known as Aadhaar, which constitutes the world's biggest biometrics bank.

The Aadhaar program, governed by the Unique Identity Authority of India (UIDAI), aims to enroll all of the country's residents through biometrics, in order to distribute 12-digit identity cards for access to social programs. So far, the program has combined enrollment of approximately 850 million people, with 630 million Aadhaar numbers generated.

The database is currently used for school attendance, natural gas subsidies to India's rural poor, and to send wages directly to people's bank accounts. The system, a landmark legacy project of India's long ruling Congress Party, also provides identification to people who do not have birth certificates.

Use Case: India

India's Universal ID program ultimately aims to provide a unique identity to all 1.2 billion residents.

Without identity documents, many individuals in India often cannot exercise basic rights and access services necessary for financial and physical security, formal employment, or democratic participation. Governments and donors cannot effectively ensure that funds reach intended beneficiaries. Universal ID allows the government to provide identification to all its residents.

With the challenge of providing identification credentials to a very large and growing population, India has opted to use biometric identification technology, rather than a card-based system, for its universal Civil ID program.

Biometric identification is considerably more accurate and secure than traditional methods of identification and authentication, and it provides an auditable trail of transactions. It offers the possibility of including individuals without documentation, such as the hundreds of millions of poor people who lack birth certificates. When combined with technology such as mobile phones, biometrics

can help streamline and facilitate payments and services in remote, underserved locations.

India's UID program is designed to be an "identity service provider" for both government programs and the private sector. Users—from pension administrators to banks—can verify people's identity against their fingerprint and Aadhaar number. When queried, the UID database returns a simple yes or no response to the match; no personal information is provided, but the beneficiaries can prove their identity.

Using multiple biometrics helps maximize accuracy, inclusion, and security. UIDAI agents collect two iris scans, 10 fingerprints, and a digital photograph from each enrollee. This multimodal system is advantageous for several reasons.

First, different biometric modalities are better at different tasks. For example, iris scans provide more data than fingerprints and are therefore more accurate for de-duplication (ensuring uniqueness), which is critical in a population as large as India's, but fingerprints are easier and cheaper to authenticate.

Second, having multiple measures is more inclusive. Many people (the elderly, manual laborers) have worn fingerprints and some have damaged eyes; using both methods reduces the failure-to-enroll rate to very low levels. Iris scans also allow younger children to enroll because the unique patterns in the eye develop and become stable before fingerprints do.

Thirdly, collecting more data upfront allows for the system to expand with population growth, and it is more cost-effective than going back to the field later because the data were insufficient or of poor quality.

The program's extensive standard-setting programs are designed to provide transparency, accountability, scalability, and technical compliance without proprietary systems that are expensive and limit innovation. This advantage creates opportunities for vendors to compete and bring down costs.

The Aadhaar case study demonstrates that using multiple biometrics helps maximize accuracy, inclusion, and security and that supporting public- and private-sector applications creates incentives for use. The Indian approach has also demonstrated that competitive, standards-based procurement lowers costs and that card-less design increases security and cuts costs but can be problematic if mobile networks are incomplete.

Social Implications

While National and Civil ID can be used to identify and verify the identity of individuals when interacting with government, it is clear that establishing clear jurisdiction and rules concerning how these systems are implemented are essential.

In the case of India, its Supreme Court ruled that Aadhaar numbers are not mandatory for receiving government services. Further, some political analysts have claimed that the establishment of the UIDAI was unconstitutional and duplicated existing population registration efforts undertaken by the Office of the Registrar General and Census Commissioner of India. As a consequence, the new incoming national government has decided to merge the Aadhaar system with the National Population Registry established for the census.

Incoming government officials in June 2014 confirmed that a merger between UIDAI and NPR would de facto occur. While the UIDAI had enrolled 63 million people in the Aadhaar database, the NPR scheme had only enrolled 25 million for national identity cards. With the new government giving precedence to the NPR due to enhanced security processes and its perceived ability to eliminate the registration of non-citizens for social benefits, it is expected that the UIDAI's role in enrolling biometrics, along with authenticating

individuals for the direct benefits scheme will end. UIDAI might survive as a "back office" operation for the national register, by providing de-duplication service, ensuring that no two people with the same biometrics are able to register multiple times.

Technical and logistical challenges also confronted Civil ID implementation in India. Recently, the Aadhaar system ran into major problems with private companies that enroll Indian citizens into the program. Private businesses engaged in Aadhaar enrollment were protesting the high penalties being levied on them by the UIDAI, due to enrollment errors. In response, the Aadhaar Enrollment Agencies Association (AEAA), the lobby group representing the businesses, warned that they will be forced to stop work across the country and seek legal action to address rising fines.

Further, several banks in India have opposed the use of Aadhaar numbers to authenticate ID before every bank transaction associated with receiving social benefits. The banks' resistance is rooted in two main concerns. Firstly, many banks want the UIDAI to bear liabilities related to false identifications, and the banks want to only use an Aadhaar solution that is interoperable with their existing systems.

Though Civil ID systems can be easily justified for emerging countries since the lack of official identity can promote a cycle of poverty and societal exclusion, countries must be mindful about how they implement such systems. While robust national identification systems stimulate social, political and economic development and can even strengthen aid delivery, they must be implemented in apolitical way, in order to be effectively implemented at all.

Developing countries must also take caution as the use of biometric identification technologies can concurrently raise serious human right concerns. Such technologies are often deployed in a legal void since constitutionally-guaranteed privacy rights are often not respected in practice. Further, sophisticated data protection safeguards are often simply not-existent in developing countries due to a lack of resources.

Biometric technology also provides the data and tools that can assist in mass surveillance and the profiling of populations. The poor regulation of biometric data can be used for unintended purposes, which can lead to discrimination. As a consequence, developing countries need to carefully plan the implementation of biometric voter enrollment systems. The most important consideration is ensuring that the enrollment process is administered independent of executive and legislative branches, and that the technology is used only for concomitant electoral or service delivery purposes. This assessment is true whether the system is being deployed in an advanced or developing country.

About the Biometrics Research Group, Inc.

Biometrics Research Group, Inc. provides proprietary research, consumer and business data, custom consulting, and industry intelligence to help companies make informed business decisions.

We provide news, research and analysis to companies ranging from Fortune 500 to small start-ups through market reports, primary studies, consumer research, custom research, consultation, workshops, executive conferences and our free daily BiometricUpdate.com news service.

Biometrics Research Group has positioned itself as the world's preferred supplier of pure-play market research and consultancy services focused on the biometric marketplace, which particular focus on the law enforcement and national security sectors. Our portfolio of white papers and full research reports is based upon high-quality quantitative analysis, allowing our clients to gain deeper understanding of the marketplace.

We customize our research design, data collection, and statistical reporting using proprietary micro- and macroeconomic modeling and regression analysis.

Through integration of our research results with qualitative analysis from our BiometricUpdate.com news service, we provide actionable business analysis.

biometrics 2014

The future of identity starts here!

21-23 October 2014 | Westminster, London UK

FULL PROGRAMME NOW AVAILABLE ONLINE

Debates | Discussion | Panel Perspectives | Unconference | Interviews | Working Groups | 65 Speakers and Panellists

Have your say and shape the future of identity at this interactive forum

- Samsung Electronics and mobility rules
- Commerical applications for banking and retail
- Fraud and cyber security
- Government projects, border management and law enforcement
- The Big Privacy Debate and building trust
- Biometrics in developing economies
- Get talking: unconference and rapid fire discussion
- Academic research and biometric innovation
- Biometrics Live: Exhibition

Keynotes from:
Home Office
Samsung Electronics
The Financial Services Club
University College London

FREE EXHIBITION **biometrics Live**

View the technologies and meet with the suppliers and integrators of biometric solutions for identity management, authentication and security

22-23 OCTOBER 2014 | FREE VISITOR REGISTRATION NOW OPEN

REGISTER BY 30 JUNE 2014 FOR REDUCED RATES

#biometrics2014
#biometricslive

Organised by: Elsevier
In partnership with: Biometrics Institute
Premier Media Partner: Biometric Update.com

www.biometrics2014.com