The Future of Biometrics

Market Analysis, Segmentation & Forecasts

Insight into the Trends, Drivers & Opportunities that will Shape the Industry through 2020

includes detailed market forecast 2009—2017

Published
August 2009

by

ACUITY
MARKET INTELLIGENCE

About Acuity Market Intelligence

Acuity Market Intelligence is the biometric industry's leading independent strategic consultancy. Acuity cuts through the clutter of information overload to provide technology-neutral and vendor-independent industry analysis for the biometrics industry and other emerging technology markets. Acuity's established reputation for candid, "hype free" insight is based on a proven record of accurately anticipating biometric and associated identification solutions market trends. Acuity relies on *rigorous intuition*—a combination of quantifiable, data driven analysis and insight honed over two decades—to consistently provide original, thought provoking, accurate, and reliable industry analysis.

The core of Acuity's knowledge base is a fundamental understanding of technology market development, technology evolution in emerging markets, and how technology is adopted and deployed most effectively in targeted vertical markets. This knowledge is applied through proven tools and techniques to help vendors, integrators, investors, and end-users:

- Identify, prioritize, and size lucrative market opportunities.
- Define and analyze targeted vertical solutions.
- Create and evaluate market development and adoption strategies.
- Achieve sustainable market dominance.
- Evaluate deployment plans within the context of generating quantifiable ROI.

Market Development Expertise

Acuity's singular focus is on the development of emerging technology markets providing expertise in the following areas:

Market Analysis – Identification and evaluation of key technological developments, market trends, industry players, and deployment effectiveness.
Opportunity Analysis – Highly granulated vertical market segmentation and identification, prioritization, and sizing of the most lucrative opportunities for a given product, service, or solution.
Solutions Analysis – Requirements and functional specifications for applications of emerging technology.
Due Diligence – Evaluation of market players to ensure:

- Opportunities have been adequately and accurately assessed.
- Financial, operational, and strategic plans are in place to create sustained market viability.
- Product and service quality can be demonstrated.

Strategic Planning – Creation of highly leveragability plans to develop, evaluate and deploy emerging technology-based solutions with the objective of achieving the highest degree of customer satisfaction and sustained market dominance.

Client Services

Clients leverage Acuity's knowledge and expertise through a range of off-the-shelf, semi-custom, and fully custom product and service offerings. These include:

Executive Briefings & Strategy Sessions – Interactive sessions provide targeted insight to Client Executives.
Consulting – Custom projects designed to support specific Client objectives.
Segment Tracking – On-going coverage of technologies, players, market drivers and dynamics of a particular industry sector or technology marketplace.
Reports – Periodic and one-off targeted analyses focused on a range of topics including: technology evolution, application development, vertical market adoption, and competitive analysis.
Research – Standard and semi-custom research projects designed to address specific industry knowledge gaps.
Workshops – One to two day intensives presenting Acuity's proprietary methodology for applying proven tools and techniques to identify, prioritize, and size market opportunities.

Please contact **Acuity Market Intelligence** for additional information
on services, availability and fee structures.

Online	www.acuity-mi.com
Phone	+1 303 449 1897
Email	info@acuity-mi.com

Report Overview

SCOPE: This report presents unique insight into how the biometrics market will evolve through 2020, what will drive and shape this market evolution, and where the most lucrative biometric market opportunities will be. This report is not a biometric primer or a comprehensive overview of the industry. ***It is an advanced strategic market analysis that requires a basic understanding of the biometrics industry and associated market dynamics and technologies.*** *The report is presented in two parts.* Part One contains the strategic analysis and Part Two provides detailed market segmentation and market-based forecasts for 2009 through 2017

OBJECTIVE: This report provides a basis for short-term, mid-range, and long-term strategic planning for technology and solution development, market investment, and phased adoption of biometrics for both Public Sector and Commercial deployments.

AUDIENCE: Individuals responsible for strategic planning, business and market development, and sales within the biometrics community including: vendors, integrators, investors, consultants, distributors, solution providers, as well as Public Sector and Commercial end-users.

METHODOLOGY: Analysis is drawn from on-going market coverage of the industry including: significant market and technical developments, tests, pilots and deployments, as well as public domain and private data sources, research and reports, surveys, and interviews with vendors, integrators, intermediaries, customers, privacy and civil liberties advocates, and other relevant technology and vertical market industry experts. Forecasts are derived from modeling total potential market opportunities for the enhancement or replacement of existing technology and non-technology based processes and solutions, and the introduction of new processes and solutions based on the unique capabilities of biometric technology. Models rely on public domain and proprietary primary data sources and are flexibly structured to account for known and predictive factors. Primary sources determine known model data. These include data points like population, population age distribution and assocated government services and benefits, number of port facilities and border control points in a given country or region, annual passports issued, the number and type of enterprises in a given country or regin, government and enterprise employment, and deployed military and civilian staff and contractors. Models are then adjusted to account for existing market conditions, current deployments, anticipated projects, and existing and planned infrastructure. Conservative assumptions for predictive factors - such as technology pricing and anticipated adoption rates – are introduced to determine forecasts. Final forecasts represent the predicted penetration of the total market value over the forecast range.

KEY CONCLUSION**:** Over the next ten years the infrastructure to enable mainstream, ubiquitous biometric authentication will be developed. Biometrics will be a fundamental embedded component of the digital world, as it becomes a key enabler of trusted transaction control – data access and flow - for personal, commercial, and government use. This trusted transaction capability will ultimately define the genuine opportunity for revenue associated with deployment of biometric technologies. The technology itself will, in many respects, become inconsequential as the applications it delivers become essential components of twenty-first century life.

COPYRIGHT AND LICENSING

This report was created by Acuity Market Intelligence for use by one individual - the purchasing party. *As such, this document is not to be reproduced and/or distributed in any electronic or printed form.* **Should the purchasing party intend to distribute this document electronically or in print for any reason, the purchasing party must contact Acuity Market Intelligence to purchase a multi-user license.** This document may, however, be shared as one would share any published single hardcopy report.

The purchasing party may reproduce and use excerpts from this report for internal purposes provided that all material is attributed to Acuity Market Intelligence and that excerpts do not substantially represent complete sections of the report or the report in its entirety.

This copyright will be strictly enforced.

AUTHOR: C. Maxine Most, Principal, Acuity Market Intelligence

Introduction

What is *The Future of Biometrics*? Strong consensus amidst well-founded apprehension indicates biometrics will become mainstream, ubiquitous technology. Opportunities abound and there has been successful initial market penetration for Physical and Logical Access, Identification Services, and Surveillance applications. From passports and ATMs to corporate network access and mobile phones, from the White Castle fast food chain and Pictet & Cie Banquiers, a renowned Swiss bank, to the Denver Rapid Transit Department Treasury and nuclear power plants, *biometric technologies are used by tens of millions of individuals across the globe for personal, commercial, and civil applications every day*. The most interesting and relevant question about the future of biometrics is not whether biometrics will prevail or even how quickly, but what is the path from today's effective but limited but use, to what most industry experts agree and most privacy and civil liberty advocates fear is biometrics ultimate destiny: *ubiquity.*

***The Future of Biometrics* provides insight into how the biometrics industry will evolve through 2020, what will drive this evolution, and where the most lucrative market opportunities will be. It is intended to provide a basis for short-term and long-term strategic planning for technology, as well as solution development and deployment for both Public Sector and Commercial applications. The report is presented in two parts. Part One contains the strategic analysis and Part Two includes market segmentation and forecasts for 2009 through 2017.**

Biometric industry revenue as defined in this report is limited to the sale, licensing, and installation of the hardware and software required to deploy biometrics as standalone solutions or integrate biometrics as part of larger identification solution. It does not include any revenue associated with the development, deployment, or integration of the non-biometric components of large-scale identification solutions.

Part One: Analysis

The first half of the report addresses fundamental questions that provide the context for developing a comprehensive view of the likely evolution of the biometrics marketplace.

- What are the Mega and Meta forces shaping the evolution of the market?
- Which industries and applications hold the most promise for biometric deployment?
- How will market demand shape technology evolution and the development of biometrically enabled solutions?
- What is the current state of the marketplace?
- How will the technology evolve and impact overall market development?
- How will the most substantial opportunities for industry players evolve?

Context

The Future of Biometrics begins with a fictional scenario representing what may prove to be a real world experience by 2020. This provides context for understanding the far-reaching implications of biometrics fully integrated into daily life.

Mega Trends

The eight global *Mega Drivers* are trends that will profoundly impact all IT development through 2020 and have important, specific implications for biometrics. They are:

- Globalization and Developing Economies
- Borderless Economies
- Workforce Decentralization and Mobility
- Population Mobility
- Proliferation of Mobile Devices and the Rise of Trusted Access Anywhere
- Central Role of Digital Identity
- Inevitability of eGovernment
- Rise of Cloud Computing

Meta Drivers

Application Solution and Technology Evolution *Meta Drivers* shape both opportunities for widespread deployment of biometrics as well as determine the technological capabilities required to address these applications.

The three key Public Sector *Application Solution Meta Drivers* are: eBorders, eID, and eGovernment.

The three key Commercial *Application Solution Meta* Drivers are: Enterprise Security, Information Transactions, Financial Transactions.

The four key *Technology Evolution Meta Drivers* are: Secure Identity Core, Secure Mobility, Secure Credentials, and Secure Transactions.

Obstacles and Opportunities

Biometric technology has the potential to enhance or threaten consumer and citizen rights and civil liberties, and exacerbate or eliminate opportunities for identity theft and fraud. Core biometric issues as well as those considered outside the direct purview of biometrics, but directly impacted by their use, are assessed relative to this inherent conflict. Central to this component of the analysis is the notion that these obstacles pose challenges that can be harnessed and transformed to provide significant opportunities for market leadership and dominance.

The State of the Market

The evolution of the biometrics market, though plagued by strange twists and turns, is on track for sustained growth. The post 9/11 promise of biometrics may not be materializing as expected; however, key applications in critical market sectors represent significant opportunities for market players who strategically focus efforts on building cost-effective solutions to business-breaking problems. Though several recent setbacks and failures of Public Sector and Commercial biometrically enabled programs have generated bad PR for the industry, *it is not the biometrics that failed*. The industry needs to move-on and continue to demonstrate the unique capabilities and ROI potential of biometrically enabled identification solutions. For both Public Sector and Commercial markets, citizen and consumer transactions may be the largest revenue generators and drivers of biometric adoption.

Future for Key Technologies

Technology evolution is inevitable and evolving capabilities and limitations will impact the relative success/ubiquity of each biometric modality. Technology convergence is also inevitable as is the emergence of multimodal biometrics as a major factor in the development of practical, ubiquitous biometric solutions. “Conventional” biometrics— AFIS/livescan, Finger. Face, Iris, Hand, Vein, Voice, Signature, Keystroke—are included in this analysis along with some of the emerging modalities. The role of multimodal biometrics and the impact of ancillary identification technologies are also discussed.

Part Two: Market Segmentation and Forecasts

The second half of the report includes market segmentation and forecasts for 2009 through 2017. A market or solution based approach is applied to the market segmentation. This is atypical in the biometrics industry where most published forecasts take a technology-based approach. This means the market segmentation in this report analyze opportunities and associated revenues in terms of geographic regions, market-based solutions, and technology applications rather than defining the size of a market based on technology revenue – e.g. the market for eBorders or Financial Transactions rather than the market for AFIS or Iris recognition. *The Future of Biometrics* approach provides data and perspective that is designed to support strategic market development planning.

Market Segmentation

The two key Application Solution domains and their associated sub domains - Public Sector (eBorders, eID, and eGovernment) and Commercial (Enterprise Security, Information Transactions, Financial Transactions) - are mapped against four key application areas— Physical Access, Logical Access, Identity Services, and Surveillance and Monitoring - to create market segmentation matrices. The resulting market segments are ranked in terms of development priority and timeframe. Each target market is also assessed in terms of the technologies (biometrics modalities) most likely to be deployed. Forecasts for the Commercial and Public Sector Application Solution domains, their sub domains, and select target markets are presented globally, by region, by technology, and by application.

Forecasts

A quantitative approach is applied to the market forecasts. This approach is based on development of scenario modeling tools designed to project total market potential for biometrically–enabled solutions within select markets. These modeling tools predict total market value based on an analysis of how biometrically-enabled solutions can augment or replace existing manual and/or automated processes, or introduce new processes based on the unique capabilities of biometrics within the given market sector and segment.

The models rely on public domain and proprietary primary data sources and are flexibly structured to account for known and predictive factors. Primary sources determine known model data. These include data points like population, population age distribution and assocated government services and benefits, number of port facilities and border control points in a given country or region, annual passports issued, the number and type of enterprises in a given country or region, government and enterprise employment, and deployed military and civilian staff and contractors. Conservative assumptions for predictive factors—such as technology pricing and anticipated adoption rates—are then introduced to determine forecasts. Final Forecasts represent the predicted penetration of the total market value over the forecast range, which in this case is 2009 through 2017

Preface to the 2009 Edition

I came across the following in an article entitled *Another day in paradise as life gets cryptic*, by Sathnam Sanghera in The Times Online on July 20, 2009.

> "The other day we got a message from our IT department at *The Times* informing us that password policy was changing as part of an annual Finance and Technology Sarbanes-Oxley audit, and that passwords must now be "eight characters long, contain a letter in upper case, a letter in lower case, a number, and a non-alphanumeric character (e.g. ?, £, %, $)". Meaning that "fluffykins", "B1 9AR" or "anotherdayinparadise" are no longer permissible and that even "BuRpy%2x" will work only for a while, as one is required nowadays to change one's password more often than you change your underpants."
>
> "I use seven passwords and passcodes to deal with my bank alone. Recent research has found that 88 per cent of employees use between five and six passwords at work. And in 2006 *The Wall Street Journal* reported that there was an insurance company where the agents needed to use 40 passwords during the average working day. The other day I spent a whole hour trying and failing, with the aid of those seven passwords, to make an online bank transfer that would have taken seconds in the days that customers had personal relationships with managers. And according to a UK survey conducted in 2004 by Microsoft, 60 per cent of computer users have at some point exhibited "anti-social behavior" in the form of shouting, "pouting in silence" and hitting computers, because of forgotten passwords"

Unfortunately, these anecdotal comments are representative of life in the twenty-first century for far too many of us. One would think the reality of these common experiences would be enough to justify and propel rampant adoption of biometrics. Sadly, this Is not true. In the two years since the original 2007 publication of this report, the industry has seen both significant accomplishments and considerable setbacks. While some major government programs have been scaled back (TWIC), are seriously behind schedule (HSPD-12 PIV cards), or have an uncertain future (UK National ID), others have been initiated (India's 1.5 billion and Mexico's 100 million strong National ID programs). Commercial investments in all non-essential IT has slowed to a crawl in the current economic climate, however, there is renewed focus on short-term ROI-based investment like time and attendance solutions. So, in spite of industry setbacks and a faltering global economy, the biometrics market remains healthy and is well positioned for steady, but slow growth.

The 2009 forecast numbers average approximately 10% below original 2007 projections for the overlapping forecast period 2009 through 2015. This adjustment is mainly due to lower than expected 2009-2010 growth attributable to stalled economy. Interestingly, while Acuity has been criticized over the last two years for underestimating the revenues projections published in 2007, most analysts have recast their projections downward during this period and have now published forecasts that are in line with Acuity's projections.

In addition to providing revised forecasts, the 2009 edition has been updated and expanded in both minor and significant ways. The elements of the market analysis that provide the context and conceptual framework stand on their own and have largely been left in tact. Minor edits and additions have been made where appropriate. For example, the Rise of Cloud Computing has been added as an eighth Mega Trend. Dated facts and relevant technical and programmatic updates have been added throughout the document as well.

A new analysis section has been added to Part One entitled "The State of The Market". This section provides insight into the current evolution of market development, provides a review of some of the of large government post 9/11 ID programs, and offers analyses of two key applications—Time and Attendance and Surveillance—and two industry verticals—Financial Services and Healthcare.

This section also takes a look at two highly visible commercial biometric business that went bust—Pay-by-Touch and the CLEAR registered traveler program. These programs together accounted for nearly half a billion US dollars in industry investment. Though each failed for their own reasons, each was doomed from their inception begging the question why is it that many small, viable biometric enterprises with great prospects for success are unable to acquire investment capital while these two ventures were able to attract significant investment with almost no chance of success?

A high-level view of the environment for market players is presented along with perspective on key developments that will impact the vendor landscape through 2020. A comprehensive competitive analysis is beyond the scope of this report and will be the subject of a follow-on report published later this year.

Finally, this section includes a discussion of the key market forecast findings from Part Two of this report. These market forecasts have been updated and greatly expanded from the original 2007 report. They now include forecasts by technology and application for the global market, for each public sector and commercial market sector, and for each region. Part Two features 29 new data tables, 27 new graphs, and 53 new charts as well as CAGR calculations for many of the existing market forecast graphs.

I hope that you find this document to be an insightful reference as you navigate the biometrics marketplace.   As always, your comments, criticisms, suggestions, questions, and complaints are welcome!

Cheers,

C . Maxine Most
Principal, Acuity Market intelligence
July 22, 2009
cmaxmost@acuity-mi.com

Table of Contents

INTRODUCTION AND OVERVIEW

EXECUTIVE SUMMARY

PART ONE: MARKET ANALYSIS

Table of Contents

PART TWO

*Regions: North America: US, CA, Mexico
EMEA: Europe, Middle East & Africa
Central and South America
Asia Pacific: Asia, Pacific Rim

Charts, Tables & Graphs—Part One

.

Charts, Tables & Graphs—Part TWO

Charts, Tables & Graphs—Part TWO

Charts, Tables & Graphs—Part TWO

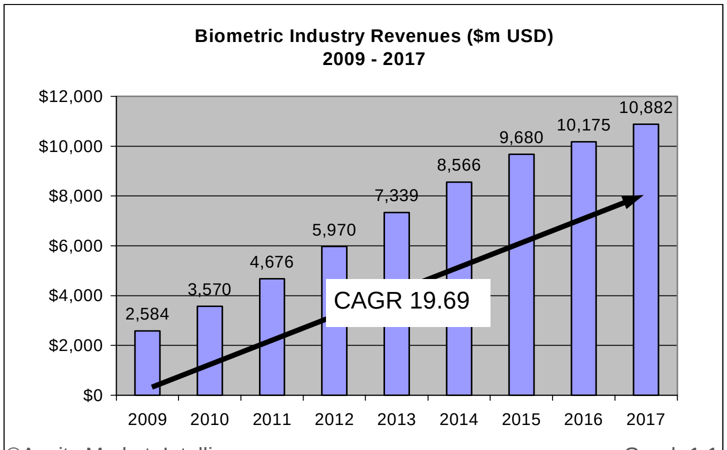
Charts, Tables & Graphs—Part TWO

Charts, Tables & Graphs—Part TWO

Executive Summary

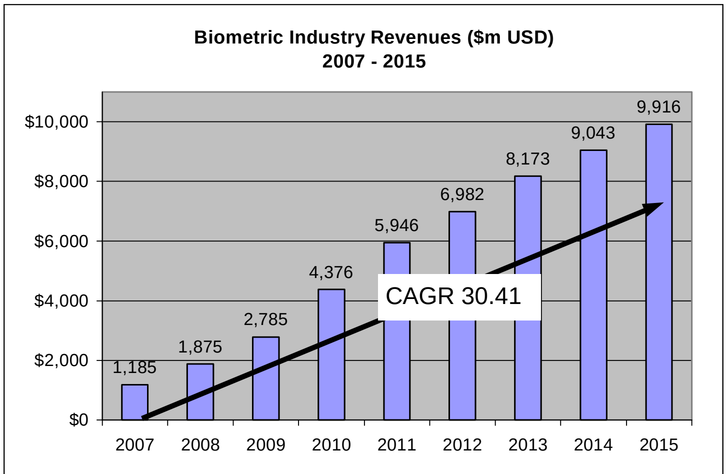
Biometric industry revenue as defined in this report is limited to the sale, licensing, and installation of the hardware and software required to deploy biometrics as standalone solutions and to integrate biometrics as part of larger identification solution. It does not include any revenue associated with the development, deployment, or integration of the non-biometric components of large-scale identification solutions.

Biometrics Industry Revenues 2009—2017



©Acuity Market Intelligence Graph 1.1

Biometrics Industry Revenues 2007—2015



©Acuity Market Intelligence Graph 1.2

Industry Overview

The biometrics industry remains on track to experience significant transformation over the next ten years. Technological capabilities will revolutionize ease of use, accuracy, and performance and greatly expand the use of biometrics for personal, commercial, and government applications. Maturing business models will evolve from product to service based offerings with the bulk of revenues generated from transaction-based opportunities.

Though there have been setbacks in a number of widely heralded biometrically enabled identification programs—the failure of the US-VISIT Exit program, the scaling back of the US Transportation Worker Identification Credential (TWIC™) program from 12 million transportation workers to one million maritime only workers (and its slow uptake even in this limited incarnation), the transformation of the UK National ID card to an opt-in program and it's potential demise based on political outcomes, and the commercial implosions of Pay-by-Touch and the CLEAR Registered Traveler offering—overall momentum in this arena continues to strengthen and will result in sustained growth opportunities.

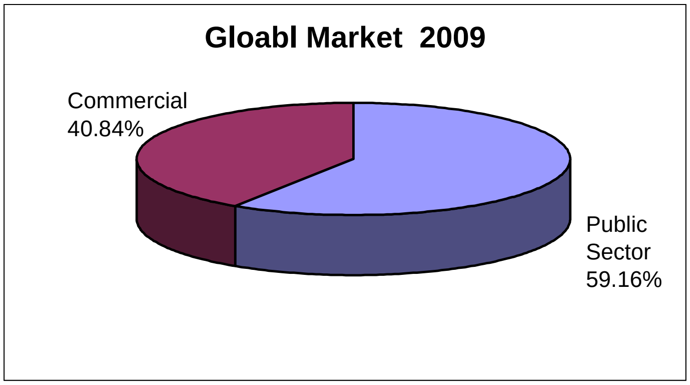
The impact of the 2008 global economic meltdown has been significant, but not devastating to the biometrics industry. Public Sector projects have slowed down and/or been scaled back. (The UK National ID may be one exception. While the state of the economy added fuel to the fire, the extreme civil liberties pushback and the political climate were the primary change agents.) Commercial opportunities have generally shifted in response to economic realities. Major IT infrastructure projects are being cancelled or postponed in favor of targeted, incremental projects that impact bottom-line performance within a 12 to 18 month window. This bodes well for biometric-based time and attendance applications, which have a proven record of providing quantifiable, short-term, ROI rather than physical or logical access solutions whose bottom line benefits are more difficult to quantify.

The overall bottom line for the biometrics industry is that there is good news and bad news. The good news: in spite of programmatic setbacks and the current worldwide economic malaise, overall identification market dynamics continue to be strong. This market environment is conducive to the level of expansion needed to realize the promise of biometrics. The not so good news: as growth continues and potential rewards increase so to will uncertainty and risk. While the inevitable outcome seems clear, the path to achieving this outcome is not. Successful navigation of this market will therefore require a clear vision and a strategic market development approach that is flexible enough to exploit opportunities created by a market in flux.

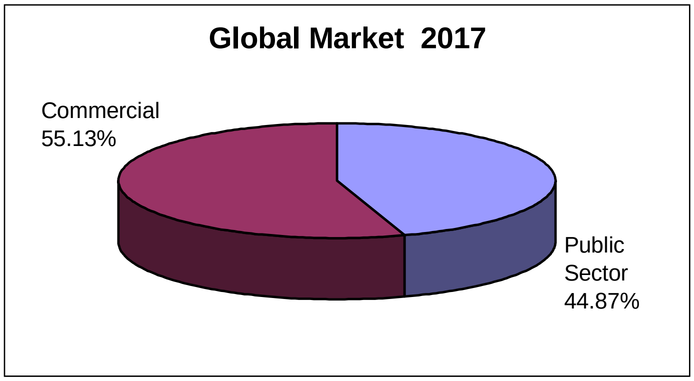
Market Growth

The market for biometrics core technology is poised for sustained growth with global revenues reaching nearly $11 billion annually by 2017 representing a CAGR of 19.69% over the forecast period. These figures are reasonably consistent with original projections made in 2007 for the 2007 to 2015 timeframe. The 2009 forecast model was updated to reflect the most recently available data and account for current market dynamics—economic and political as well as technical. Slower growth than originally anticipated in the 2009 to 2012 timeframe, due to the faltering economy, is balanced out by slightly stronger growth in the 2012 to 2015 timeframe. The result—projections that reach roughly the same revenue levels by 2015, but with a lower overall anticipated CAGR of 20% from 2009 through 2017 rather than the higher CAGR of 30% for 2007 through 2015 that was forecast in 2007.

Biometrics Industry Market Share: Public Sector vs. Commercial 2009 and 2017



©Acuity Market Intelligence Chart 1.3



©Acuity Market Intelligence Chart 1.4

Major Research Findings

Over the next ten years the infrastructure to enable mainstream, ubiquitous biometric authentication will be developed. This infrastructure will both enable and be driven by true mass public deployment of biometrics for personal, commercial, and government applications representing the emergence of a new era of biometrics. As biometrics become a critical embedded component of the digital world, it will be a key enabler of trusted transaction control – data access and flow—for all IT systems. This secure transaction capability will ultimately define the genuine opportunity for revenue associated with deployment of biometric technologies.

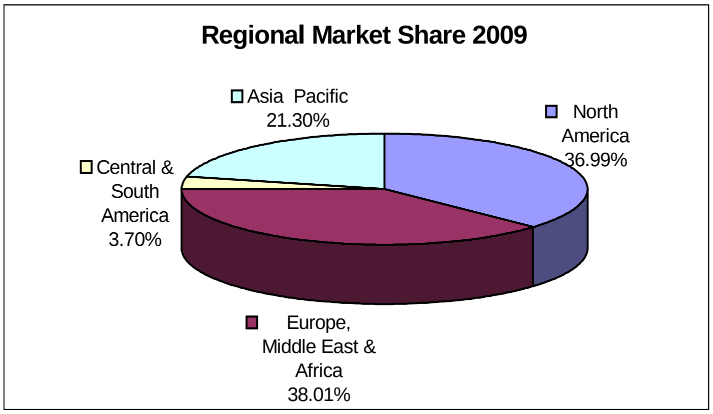
Key Forecasts

- Commercial deployment revenues match Public Sector revenues by 2014 and then surpass Public Sector revenues by 2017 representing growth form nearly 41% to just over 55% of the total global market for biometrics core technology. The Public Sector revenue share declines form 59% to 45% over the period. The comparative CAGRs reflect this shift in market dominance as Public Sector grows as a respectable 16% while the Commercial marketplace grows at a much faster pace reaching 24% CAGR over the forecast period..

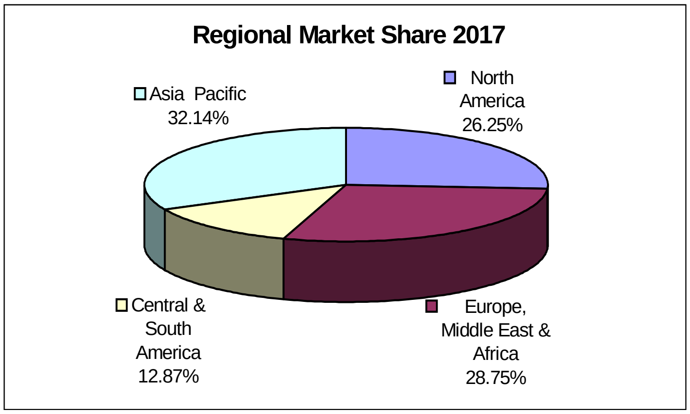
- The sectors with the highest CAGRs within the Public Sector and Commercial arenas are eGovernment with 42% and Information Transactions at 50%. The other sectors CAGRs are as follows: eBorders 10%, eID 12%, Enterprise Security 12%, and Financial Transactions 37%.

- Revenue growth rates vary significantly across regions. The Central and South American region will experience the highest CAGR over the forecast period of 39.46% while growing form nearly 4% to nearly 13% of total global revenues. Overall market dominance will shift from Europe (and the greater EMEA region) and the US (and the greater North America region) to Asia (and the greater Asia Pacific region). North America and EMEA's percentages of total global revenues will decrease over the forecast period from 37% to 26% and 38% to 29% respectively with associated modest CAGRs of 15% and 16%. By 2017, the Asia Pacific Region will generate the greatest percent of revenues for the biometrics industry with more than 32% of global revenues growing at a CAGR of 26%.

Market Share by Region 2009 and 2017



©Acuity Market Intelligence Chart 1.5



©Acuity Market Intelligence 2007 Chart 1.6

Context

This fictional scenario of a typical “day in the life” routine anticipates some of the ways that biometrics may be embedded in our lives by the year 2020. While this is an extreme rather than accurate representation of the future, this glimpse of possibility provides a context for considering how the biometrics industry must evolve in terms of technology, usability, infrastructure (technical, legal, and social), and business models for the promise of biometrics to be realized.

Biometrics in 2020: A Day in the Life ...

7:00 am Personalized voice-based alarm bids you a good morning and waits for your response to verify identity and provides details of overnight communications (phone, video, email, text) per your personal settings. Room lighting adjusts and the morning news broadcasts as you rise from bed.

7:30 am Your personal environmental settings (messaging, media, lighting) follow you from the bedroom and are activated as you enter the kitchen. Once again your voice commands are used to verify identity. You continue to review any important messages and place an overseas call to confirm an international business transaction. An iris image captured from your PDA authorizes the transaction.

8:15 am Your automobile senses your approach, verifies car access via RFID broadcast from the smart card in your PDA, unlocks the door, and confirms identity though scan of your fingers and palm as you grip the handle of the door and the steering wheel. As you drive, your voice activated PDA interface access provides a third confirmation of identity enabling you to attend to several personal matters—securing your mortgage payment, reviewing the results of a recent medical exam, and ordering flowers for your spouse.

9:00 am You arrive at a government client site where facial recognition confirms you are not on any watchlist as you enter the building and your government contractor PIV compatible ID credential embedded in your PDA grants access to client facilities and IT systems. Your touch screen PC captures dynamic signatures as you complete a new contract which is then encrypted and distributed electronically to the legal, contract, and sales departments of your and your client's organization.

Noon As you approach an ATM your identity is confirmed via iris recognition and you withdraw $100. You are meeting a friend for lunch and your favorite family owned diner prefers cash.

1:15 pm You pull up the driveway and the garage door opens in response to your car transmitting it’s vehicle ID along with a confirmation of you being the operator of the vehicle via an encrypted RFID signal. You enter your secure home/office. Motion detection triggers facial identity confirmation, the lights and temperature are adjusted to your personal preferences, and the computer is turned on with your personal settings. As you sit in your desk chair iris recognition confirms your identity and you are simultaneously granted access to your company’s network and appropriate applications and files.

3:00 pm You log off your company's network and check bank balances, pay a few bills, and send a biometrically signed document via email to complete your mortgage refinancing contract. Your computer captures fingerprints, keystroke dynamics, and iris images to allow you to access accounts, complete transactions, and send secure email.

4:30 pm You arrive at a client meeting with representatives of the Department of Transportation at the city airport. Unfortunately, you experience a delay clearing facility security, as the TWIC system and the PIV system are still not communicating well with each other. Your review of the latest upgrades to the Registered Traveler system indicates throughput continues to increase with enrollment now stabilized at roughly 85% of local frequent travelers. The fully automated enrollment stations capturing face, iris and ten-print slaps have been effectively integrated with Passport, DMV, and FBI databases anonymously approving or rejecting candidates. The upgrades have been well received and have successfully resolved both front and back-end usability issues freeing up TSA staff from full-time monitoring responsibilities.

7:00 pm A quick trip to the supermarket on the way home to pick up a few items. You fill your cart and walk through the fast purchase lane. Each of your items is scanned and your bank account charged via a fused facial and iris recognition authorization tied to the smart card in your PDA as you roll your cart through without stopping.

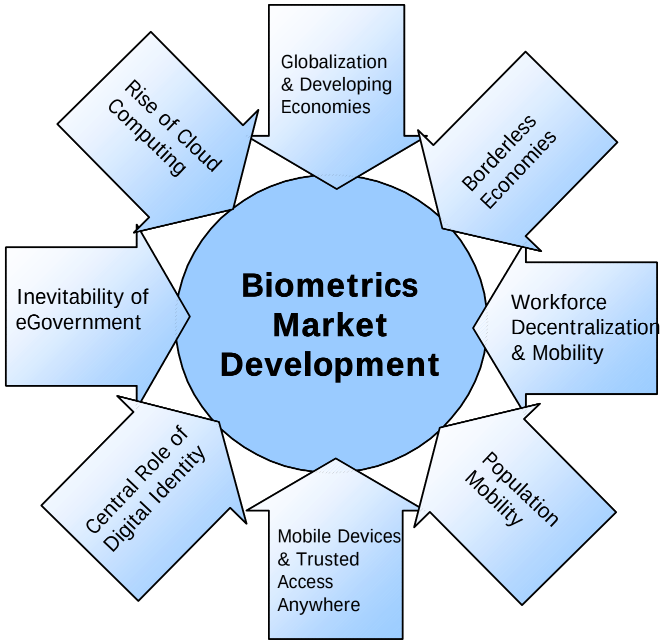
8:00 pm Your presence is detected in the entertainment room and identity confirmed through a facial image as you are asked which of your favorite programs you would like to view. Your incoming messages are held and you settle down to watch as you are reminded that it is garbage night.

10:50 pm As you enter the bedroom, the lights adjust and you are alerted to one non-critical message waiting for you. You leave it until morning and your identity is confirmed as you issue the voice command override your scheduled 11:00 pm sleep settings.

Mega Trends

Critical global trends impacting the requirements and associated development of worldwide IT solutions will have profound implications for the biometrics industry. These *Mega Trends* (Chart 1.8) will continue to drive the adoption of identity-centric, service-based IT models that rely on the trusted linkage of individuals with established identities to specific physical and logical privileges, access, and tasks. Biometrics are a key enabling component of the authentication infrastructure required to support this type of trusted linkage. Therefore, the evolution of these Mega Trends and the IT market demand they create, are integrally linked to the evolution of the biometrics marketplace.

Mega Trends


Biometrics Market Development
Globalization & Developing Economies
Borderless Economies
Workforce Decentralization & Mobility
Population Mobility
Mobile Devices & Trusted Access Anywhere
Central Role of Digital Identity
Inevitability of eGovernment
Rise of Cloud Computing

©Acuity Market Intelligence Figure 1.1

1) Globalization and Developing Economies

The nature of commerce and information and resource sharing are in the process of a fundamental transformation. The interconnected networks—human and technology—that are making this transformation possible will continue to increase in complexity and capacity as the nature and volume of information, goods, and services being shared continues to grow. This growth means ever increasing reliance on technology processes that must be reliable, transparent, and secure. The ability to bridge the gap between individuals and their digital identities make biometrics not only a perfect fit but an absolute requirement to sustain this level of trusted digital connectivity.

The on-going evolution of Developing Economies will continue to increase the size and scope of local and global markets. Many of these market environments are skipping twentieth century style industrialization and progressing directly to information based economies. This type of expanding commerce will require stringent authorization and authentication as critical goods and services originate from and are delivered to locations across the globe that lack established and trusted political and economic infrastructures. Whether it is a help desk in India, a parts manufacturer in China, a software engineer in Venezuela, or a consultation with a medical specialist in South Africa, organizations traversing the digital world will no longer have a choice about tightly controlling their environments. The notion of security based on a bounded environment—physical or logical—must give way to a digital world controlled through the use of identity. “Who goes there?" and “What do you have access too?” will become the keys to trusted communication and transactions that drive twenty-first century global trade and economic development.

2) Borderless Economies

The notion of Borderless Economies is nothing new. However, the realization of the concept has accelerated over the last ten years by the near ubiquity of the Internet for personal, commercial, and government use. This is particularly true in the Financial Services arena where near instantaneous access to global transactions has created an unprecedented global financial community. While Globalization and it’s associated “off shoring” of manufacturing, technical development, and a range of other business and consumer services are impacting the development of Borderless Economies, an expanding European Union and trade agreements such as NAFTA and CAFTA are breaking down traditional physical and logical borders.

Unfortunately, free flowing global 24/7 trade is on a direct collision course with urgent 21st century security requirements at ports and borders and in cyberspace. The ideal of unencumbered movement of goods and services across the globe came to a rather existential halt post 9/11. The magnitude of the potential threat posed by a world with no borders was suddenly recognized both in the physical and virtual realms.

To date, limited safeguards have been put into place to combat these threats. Some improvement in process and technology has been applied to tracking and monitoring people and the transportation and management of good and containers. Increased logical security and surveillance has also been initiated. However, over the next several decades there will be continued efforts to balance the desire for seamless movement of goods and services with the acknowledgement that physical and logical borderless access pose genuine threats. The identification, authorization, and authentication of individuals involved in accessing everything from port facilities, shipped goods and containers, to manifests, data bases, personnel files, and computer systems must be a central component of providing a secure Borderless Economy.

Meta Drivers

Application Solution Meta Drivers

The Application Solution Meta Drivers are market demand drivers that define a framework for identifying the most lucrative market opportunities. The biometrics industry can be broadly divided into two major Application Solution domains-—Public Sector and Commercial—where each domain has three key Meta Drivers. This framework is not comprehensive in reflecting every possible market opportunity, but rather focuses on key growth markets for biometrically enabled solutions in their respective Application Solution domains. Charts 1.9: Public Sector Meta Drivers (below) and Chart 1.10: Commercial Meta Drivers (next page) show the demand curves for each of the key Meta Drivers. Demand curves indicate the relative intensity of market demand of a given product, service or solution over a given period of time. While they generally parallel the growth curve of a market, they do not quantify actual revenue for the specified Market.

Public Sector Meta Drivers

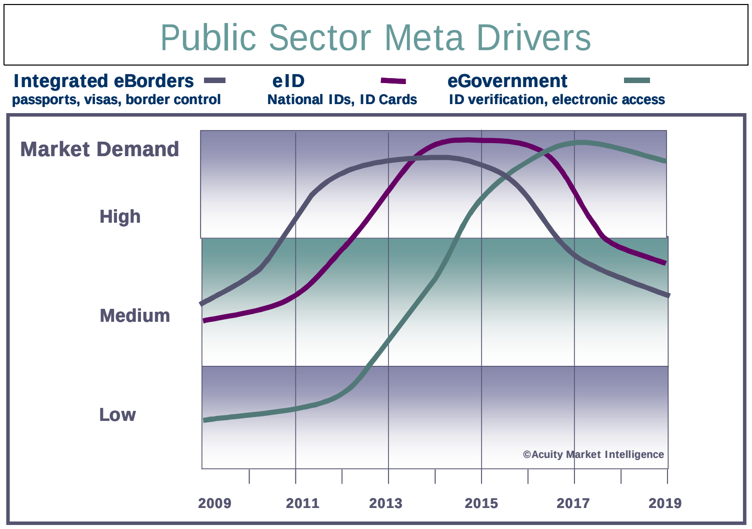


Chart 1.11

The three key Public Sector Application Solution Meta Drivers are: 1) Integrated eBorders—the full scope of electronic and automated border control management including travel documents, transportation worker IDs, vehicle access, immigrant Visas and IDs, and expedited passenger systems, 2) eID—includes civil and criminal ID, national and other identity cards, benefits distribution, voter registration, drivers licenses, criminal identification, and other physical and virtual credentials, and 3) eGovernment—fully transactional interactive service delivery for citizens and commercial entities.

The three key Public Sector Meta Drivers are integrally linked. They demonstrate a high-level sequential dependence. Learnings from the development of solutions in eBorders enables the development of solutions for eID which will lay the groundwork for the development of interactive eGovernment services. Public sector ID solutions will therefore progress from highly targeted groups of participants —e.g. expedited air travelers—to broader based groups—e.g. recipients of government healthcare services—and finally to citizen-wide applications—e.g. citizen access to electronic government/ services.

Post 9/11, 3/11, 7/7 terrorist fears acelerate the deployment of US-VISIT and other biometrically-enabled international border control systems. The initial eBorders demand peak has already begun in Europe and the US and will remain in force through 2013. The subsequent demand curve for eID solutions–which benefits from the systems architected for use in integrated eBorders applications–peaks around 2015. Demand for eGovernment will lag sustaining peak demand around 2017 as the authentication implications of large-scale, transactional eGovernment systems are recognized and solutions implemented. As millions of citizens worldwide rotuinely rely on biometrically-enabled identification to travel, identify themselves in various ways, and interact and transact with local, regional and federal governments, human-machine authentication will become an integral component of twenty first century government operations.

eBorders: Post 9/11 eBorders initiatives were introduced to identity unwanted individuals and prevent them from entering sovereign nations. They have been expanded to include expediting low security threat travelers via automated border control systems in Europe, Australia, the US, and the Middle East.   To date, there has been a near exclusive focus on managing the “front end” of the border control problem—moving travelers across borders. This includes the issuance of roughly $100 million ePassports worldwide. However, in many respects the “back end” of the problem such as background and ID checks on staff, crew and third-party employee facility access, securing tarmac, shipping lanes, and vehicle access, and protecting the corresponding IT infrastructures pose larger, potentially more dangerous security threats. While there is significant demand in this area, it is likely that sustained growth will occur at a measured pace as countries across the globe continue to develop and deploy customized eBorders solutions.

eID: There are ten EU nations with existing National ID programs. Another thirteen in development, and recently both India (populations 1.8 billion, and Mexico (population 110 million) have announced pans to issue biometrically enabled National IDs. There is even discussion in the US giving citizens the “option” of having a biometrically enabled Social Security card. One of the key issues for any type of electronic identification program is the reliability of the originating documentation and the process used to establish initial ID. In many cases, initial identification is based on documents and processes that are woefully inadequate for establishing a “trusted” identity. This creates the potential for validating and integrating identities that may have been acquired fraudulently. Establishment of an initial, non-reputable identity is key to a reliable, comprehensive identity program. However, managing this risk within the constraints of data protection and civil liberties legislation is no small challenge. Biometrics are an essential element of this proc-

State of the Market

The NEW STATE of the Biometrics Market

The market for biometrics is in a strange state and will most likely not follow the typical path of disruptive technology adoption. Biometrics have been considered a disruptive innovation on the verge of breakthrough for an extended period of time. Post 9/11 security concerns that were meant to propel the biometrics market forward, created an even greater expectation of rapid market acceleration that never materialized.

In terms of classic emerging technology adoption as defined by Geoffrey Moore in his high-technology market development bible, "Crossing the Chasm", this translates into an expectation of rapid *Chasm Crossing* from early to mainstream markets, followed by a phase of highly targeted and leveraged *Bowling Alley* market development, progressing to a period of nearly insatiable market demand— the *Tornado*. Instead, over the past few years the market has essentially passed over the Chasm and stalled out. This is due to two critical factors: 1) the failure of technologies to deliver promised capabilities, and 2) the failure of market players to develop complete, commercially viable solutions to targeted business-breaking problems based on currently available technology capabilities.

There has been far too much infatuation with the belief (wish?) that large government contracts – not targeted commercial opportunities – would be the engine driving rapid market expansion. Progress on the government front has been substantial, but has not provided the scale of opportunity necessary for the industry to thrive. The result: market players—with few noteworthy exceptions—have failed to leverage the classic target market development phase of the adoption lifecycle to produce commercially viable, proven solutions which would then be directly applicable to large-scale ID systems.

This has created a market dynamic where biometrics as a class of disruptive or discontinuous technology has not moved completely through its revolutionary market development cycle and yet is now subject to significant evolutionary or continuous innovation. In other words, just as biometrics are beginning to stabilize and deliver on past promises, current expectations continue to be driven by “next generation” technologies.

While there is now clear industry momentum towards solutions development, the *market making* opportunity has passed. The industry is no longer in a position to define the marketplace but rather is increasingly subject to *very specific* market driven requirements and customer demands. It is therefore likely that market will experience linear growth rather than the exponential growth most readily associated with Moore's technology lifecycle. Rather than the typical "hockey stick" curve of recent innovations such as mobile phones or the Internet, biometrics adoption will mimic the growth curve of ATMs, which achieved roughly 80% adoption through linear growth over a period of 20 years.

This has significant strategic market development implications. In a classic market development scenario, target market penetration precedes concern with larger opportunities. This is the process of developing dominant category positioning to leverage the ensuing "Tornado" phase. However, given the current state of the marketplace, biometrics players—across the value chain—must simultaneously manage progress towards expansion into large looming market opportunities while rigorously and systematically building a target penetration strategy. The industry must relinquish the mantle of disruption innovation and focus on *truly delivering* on the promise of biometrics by providing working solutions to real problems based on existing capabilities. *Biometrics that actually work*.

Post 9/11 Government Bonanza – Taking Stock

The post 9/11 promise of biometrics was integrally linked to a series of initiatives proposed by the US and other governments beginning in late 2001 and 2002. 9/11 essentially provided the impetus for biometrically enabled ID programs in the US and across the globe. Existing ID initiatives were given a strong boost and new initiatives were developed to create more reliable and secure identification documents, programs, and processes. Industry vendors, integrators, pundits, and the investment community were whipped up into a near hysterical frenzy believing this to be the basis of an on-going, thriving, biometrics marketplace. Nearly eight years later, the dust long settled, expectations have been greatly scaled back *as* these initiatives have varied significantly in the success they have achieved.

US-VISIT seems likely to remain an entry only program as multiple attempts to create the exit portion have failed. Registered Traveler (RT), once touted as “an enhanced security program” for frequent fliers, was scaled back to a cut-to-the-front-of-the-line opportunity whose future crashed with the abrupt collapse of Verified Identity Pass’s CLEAR program in June 2009. Just prior to CLEAR’s demise, the US House of Representatives passed a bill to reinstate the TSA background checks for RT. However, given the status of CLEAR and the long list of legislative priorities, it is unlikely the US Senate’s companion bill can be expected any time soon. Meanwhile, The latest “potential” biometrics boon is wrapped around the illegal immigration debate. There is discussion in the Senate of creating a biometric identification for all US workers—a smart Social Security card?. This will no doubt receive much hoopla in the biometrics industry and be the subject of grandiose plans. However, it is just as likely to face the kind of obstacles thrown up over REAL-ID and be subject to the type of scaling back the TWIC program experienced.