The Future of Biometrics

Market Analysis, Segmentation & Forecasts

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

May 2007

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 insight and analysis for the biometrics industry and other emerging technology markets. The core of Acuity's knowledge base is 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 & size lucrative markets.
- Define & analyze targeted vertical solutions.
- Create & evaluate market development and adoption strategies.
- Achieve sustainable market dominance.
- Evaluate deployment plans within the context of generating *real* 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 or service
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 and 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 forecasts through 2015.

OBJECTIVE:

This report provides a basis for short, 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 applications.

AUDIENCE:

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

METHODOLOGY:

Analysis is drawn from on-going market coverage of industry milestones, developments, announcements, presentations, 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 based on 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 evolving technology. Conservative adoption rates are then applied for given market sectors and applications to determine market value. .

KEY CONCLUSION:

Over the next 10 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 21st 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 form for any other reason than their own personal use, 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 excerpted material from this report for internal purposes provided that all material is attributed to Acuity Market Intelligence and that excerpts do not substantially represent 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 trepidation indicates biometrics will become mainstream, ubiquitous technology. Opportunities abound and to date there has been significant market penetration in the areas of identify confirmation and credentialing, physical and logical access, and surveillance. From passports and ATMS to corporate network access and mobile phones, from White Castle and Pictet & Cie Banquiers, a renowned Swiss bank, to the Denver RTD (Rapid Transit Department) Treasury, biometric technologies are used by hundreds of thousands of individuals across the globe for personal, commercial, and civil applications every day. The most interesting and relevant questions about the future of biometrics are not so much about if biometrics will prevail or even how quickly, but rather what is the path from today's limited and relatively obscure—though effective—use to what most industry experts agree and most privacy advocates and civil libertarians 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 and long term strategic planning for technology and 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 through 2015.**

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?
- 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 very real world experience in the year 2020. This provides context for understanding the far-reaching implications of biometrics as an integral component of daily life.

Mega Trends

The seven 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 the Development of the Third World
- 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

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

Biometrics technology has to the potential to enhance or threaten consumer and citizen rights, privacy and opportunities for identity theft and fraud. Core biometric issues as well as those considered outside the 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.

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**.**

- AFIS 10 Print
- Iris
- Voice
- Finger
- Hand
- Signature

?Face

- Vein
- Keystroke

<u>Part Two: Market Segmentation and Forecasts</u>

The second half of the report includes market segmentation and forecasts through 2015.

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 Confirmation and Surveillance - to create market segmentation matrices. The resulting markets 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 and by region.

This segmentation approaches the marketplace conceptually rather than along specific industry lines. The reasoning behind this approach is based on market development strategy that emphasizes incremental market growth as a means to achieving market dominance. A product or service is proven within an initial target market and then sequentially introduced and proven in individual markets within a group of closely aligned target markets. These target groupings often lie within a vertical industry. However, in the case of biometrics, they cross traditional industry boundaries and are more solutions focused e.g. a total identification solution for international airports includes employee logical access, vehicle access, travel documents, expedited passengers, perimeter security, and facility surveillance. Therefore, the segmentation in this report allows for selection of a group of markets within a specific Application Solution Domain rather than in a more traditional industry classification such as Travel, Transportation, Government, Law Enforcement, Healthcare, Financial Services etc.

Forecasts

A quantitative approach is applied to market forecasts. This approach is based on the 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 unique technological capabilities within the market.

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—such as the number of port facilities or annual passports issued. 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, 2007 through 2015

Table of Contents

PART ONE

Executive Summary (Analysis & Forecasts) **1.1**
Market Growth 1.1
Mega Trends 1.1
Meta Drivers 1.1
Solution Adoption Framework 1.2
Obstacles/ and Opportunities 1.2
Future for Key Technologies 1.3
Market Segmentation 1.3
Major Research Findings 1.4
Context **1.6**
Biometrics in 2020: A Day in the Life
Mega Trends **1.7**
Globalization Third World Development 1.7
Borderless Economies 1.7
Workforce Decentralization and Mobility 1.7
Population Mobility 1.8
Proliferation of Mobile Devices and the Rise of Trusted Access Anywhere 1.8
Central Role of Digital Identity 1.8
Inevitability of eGovernment 1.9
Meta Drivers **1.10**
Public Sector *Application Solution Meta Drivers* 1.10
- eBorders, eID, and eGovernment. 1.10

Commercial *Application Solution Meta Drivers* 1.11
- Enterprise Security, Information Transactions, Financial Transactions. 1.11

Technology Evolution Meta Drivers 1.12
- Secure Identity Core, Secure Credentials, Secure Transactions, & Secure Mobility 1.12

Obstacles and Opportunities **1.13**
Countervailing Forces 1.13
- Opportunity Threat Dichotomy 1.13
Privacy, Centralized Databases, Single View of Identity, Identity Theft/Fraud

Core Issues 1.14
- Bridging the Human-Machine Identity Gap: 1.14
Enrollment, Human Factors, Privacy/Civil Liberties
- Solutions Development: 1.15
Extensible Security, Context Specific Identity, Price/Performance, Interoperability

Future for Key Technologies **1.16**
Capabilities and Limitations Impacting Ubiquity of Biometric Modalities 1.16
- AFIS/10 Print 1.16
- Finger 1.16
- Face 1.16
- Iris 1.16
- Hand 1.17
- Vein 1.17
- Voice 1.17
- Signature 1.17
- Keystroke 1.17
- Other `` 1.17

Impact and Role of Multimodal Solutions 1.18
Impact of Related Technology Development 1.18
Analysis Conclusions 1.20

Table of Contents

PART TWO

Introduction to Segmentation and Forecasts 2-1

- Methodology 2.1
- Data Sources 2.1
- Model Assumptions./Constrains 2.1
- Market Segmentation 2.1

Market Segmentation 2-2

- Public Sector: eBorders, eID, eGovernment 2.2
  - - Target Markets 2.2
  - - Development Priority 2.3
  - - Solutions Timeframe 2.3
  - - Technology Deployment 2.3
- Commercial: Enterprise Security, Information Transactions, Financial Transactions 2.4
  - - Target Markets 2.4
  - - Development Priority 2.5
  - - Solutions Timeframe 2.5
  - - Technology Deployment 2.5

Market Forecasts 2-6

- Global Market 2.6
- Public Sector - Global, Regional*, EU, US 2.9
- Public Sector by Solution 2.12
  - - eBorders - Global, Regional, EU, US 2.12
  - - eBorders Key Targets- Global, EU, US 2.15
  - - eID - Global, Regional, US, EU 2.16
  - - eID Key Targets- Global, EU, US 2.19
  - - eGovernment - Global, Regional, EU, US 2.20
  - - eGovernment Key Targets- Global, EU, US 2.23
- Commercial - Global, Regional, EU, US 2.24
- Commercial by Solution 2.27
  - - Enterprise Security - Global, Regional, EU, US 2.27
  - - Enterprise Security Key Targets- Global, EU, US 2.30
  - - Information Transactions - Global, Regional, EU, US 2.31
  - - Information Transactions Key Targets- Global, EU, US 2.34
  - - Financial Transactions - Global, Regional, EU, US 2.35
  - - Financial Transactions Key Targets - Global, EU, US 2.38
- Regional 2.39
  - - North America: Key Public Sector and Commercial Markets 2.39
  - - EMEA: Key Public Sector and Commercial Markets 2.40
  - - Central and South America: Key Public Sector and Commercial Markets 2.41
  - - Asia Pacific: Key Public Sector and Commercial Markets 2.42

Forecast Conclusions 2-43

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

Charts, Tables & Graphs—Part One

.

Graph 1.1: Biometrics Industry Revenue 2007—2015 ____ 1.1
Chart 1.1: Solution Adoption Framework ____ 1.2
Chart 1.2: Public Sector Market Segmentation ____ 1.3
Chart 1.3: Commercial Market Segmentation ____ 1.4
Chart 1.4: Worldwide Market 2007: Public Sector vs. Commercial ____ 1.4
Chart 1.5: Worldwide Market 2015: Public Sector vs. Commercial ____ 1.4
Chart 1.6: Biometrics Industry Market Share 2007 by Region ____ 1.5
Chart 1.7: Biometrics Industry Market Share 2015 by Region ____ 1.5
Graph 1.2: Public Sector Markets Revenue 2007—2015 ____ 1.5
Graph 1.3: Commercial Markets Industry Revenue 2007—2015 ____ 1.5
Chart 1.8: Mega Trends ____ 1.7
Chart 1.9: Public Sector Application Solution Meta Drivers ____ 1.10
Chart 1.10: Commercial Application Solution Meta Drivers ____ 1.11
Chart 1.11: Technology Evolution Meta Drivers ____ 1.12
Chart 1.12: Opportunity Threat Dichotomy ____ 1.13
Chart 1.13: Core Issues Map ____ 1.14
Chart 1.14: Solutions Value Chain ____ 1.15
Chart 1.15: Global Market by Technology 2007 ____ 1.17
Chart 1.16: Global Market by Technology 2015 ____ 1.17
Chart 1.17: Future of Key Technologies ____ 1.19
Chart 1.18: Transformation Components ____ 1.20

Charts, Tables & Graphs—Part TWO

.

Chart 2.1: Public Sector Market Segmentation 2.2
Chart 2.2: Public Sector Development Priority 2.3
Chart 2.3: Public Sector Solutions Timeframe 2.3
Chart 2.4: Public Sector Technology Deployment 2.3
Chart 2.5: Commercial Market Segmentation 2.4
Chart 2.6: Commercial Development Priority 2.5
Chart 2.7: Commercial Solutions Timeframe 2.5
Chart 2.8: Commercial Technology Deployment 2.5
Graph 2.1: Biometrics Core Technology Total Market 2.6
Table 2.1: Biometric Core Technology and Value Chain Forecast 2.6
Graph 2.2: Biometric Core Technology and Value Chain Forecast 2.6
Table 2.2: Global Market by Region 2.7
Graph 2.3: Global Market by Region 2.7
Chart 2.9: Market Share by Region 2007 2.7
Chart 2.10: Market Share by Region 2015 2.7
Table 2.3: Public Sector versus Commercial 2.8
Graph 2.4: Public Sector versus Commercial 2.8
Chart 2.11: Public Sector versus Commercial 2007 2.8
Chart 2.12: Public Sector versus Commercial 2015 2.8
Table 2.4: Public Sector Market Forecast - Global 2.9
Graph 2.5: Public Sector Market Forecast - Global 2.9
Table 2.5: Public Sector Market Forecast - By Region 2.9
Graph 2.6: Public Sector Market Forecast - By Region 2.9
Graph 2.7: Public Sector Market Forecast - North America 2.10
Graph 2.8: Public Sector Market Forecast - EMEA 2.10
Graph 2.9: Public Sector Market Forecast - Central and South America 2.10
Graph 2.10: Public Sector Market Forecast - Asia Pacific 2.11
Graph 2.11: Public Sector Market Forecast - EU 2.11
Graph 2.12: Public Sector Market Forecast - US 2.11
Table 2.6: eBorders Market Forecast - Global 2.12
Graph 2.13: eBorders Market Forecast - Global 2.12
Table 2.7: eBorders Market Forecast - By Region 2.12
Graph 2.14: eBorders Market Forecast - By Region 2.12
Graph 2.15: eBorders Market Forecast - North America 2.13
Graph 2.16: eBorders Market Forecast - EMEA 2.13
Graph 2.17: eBorders Market Forecast - Central and South America 2.13
Graph 2.18: eBorders Market Forecast - Asia Pacific 2.14
Graph 2.19: eBorders Market Forecast - EU 2.14
Graph 2.20: eBorders Market Forecast - US 2.14
Table 2.8: Expedited Traveler Market Forecast - Global, EU, US 2.15
Graph 2.21: Expedited Traveler Market Forecast - Global, EU, US 2.15
Table 2.9: Port Facility Market Forecast - Global, EU, US 2.15
Graph 2.22: Port Facility Market Forecast - Global, EU, US 2.15

Charts, Tables & Graphs—Part TWO

Table 2.11: eID Market Forecast - Global 2.16
Graph 2.24: eID Market Forecast - Global 2.16
Table 2.12: eID Market Forecast - By Region 2.16
Graph 2.25: eID Market Forecast - By Region 2.16
Graph 2.26: eID Market Forecast - North America 2.17
Graph 2.27: eID Market Forecast - EMEA 2.17
Graph 2.28: eID Market Forecast - Central and South America 2.17
Graph 2.29: eID Market Forecast - Asia Pacific 2.18
Graph 2.30: eID Market Forecast - EU 2.18
Graph 2.31: eID Market Forecast - US 2.18
Table 2.13: Civil ID Market Forecast - Global, EU, US 2.19
Graph 2.32: Civil ID Market Forecast - Global, EU, US 2.19
Table 2.14: Government Admin ID Market Forecast - Global, EU, US 2.19
Graph 2.33: Government Admin ID Market Forecast - Global, EU, US 2.19
Table 2.15: eGovernment Market Forecast - Global 2.20
Graph 2.34: eGovernment Market Forecast - Global 2.20
Table 2.16: eGovernment Market Forecast - By Region 2.20
Graph 2.35: eGovernment Market Forecast - By Region 2.20
Graph 2.36: eGovernment Market Forecast - North America 2.21
Graph 2.37: eGovernment Market Forecast - EMEA 2.21
Graph 2.38: eGovernment Market Forecast - Central and South America 2.21
Graph 2.39: eGovernment Market Forecast - Asia Pacific 2.22
Graph 2.40: eGovernment Market Forecast - EU 2.22
Graph 2.41: eGovernment Market Forecast - US 2.22
Table 2.17: Citizen Facing Market Forecast - Global, EU, US 2.23
Graph 2.42: Citizen Facing Market Forecast - Global, EU, US 2.23
Table 2.18: Commercial Facing Market Forecast - Global, EU, US 2.23
Graph 2.43: Commercial Facing Market Forecast - Global, EU, US 2.23
Table 2.19: Commercial Market Forecast - Global 2.24
Graph 2.44: Commercial Market Forecast - Global 2.24
Table 2.20: Commercial Market Forecast - By Region 2.24
Graph 2.45: Commercial Market Forecast - By Region 2.24
Graph 2.46: Commercial Market Forecast - North America 2.25
Graph 2.47: Commercial Market Forecast - EMEA 2.25
Graph 2.48: Commercial Market Forecast - Central and South America 2.25
Graph 2.49: Commercial Market Forecast - Asia Pacific 2.26
Graph 2.50: Commercial Market Forecast - EU 2.26
Graph 2.51: Commercial Market Forecast - US 2.26
Table 2.20: Enterprise Security Market Forecast - Global 2.27
Graph 2.52: Enterprise Security Market Forecast - Global 2.27
Table 2.21: Enterprise Security Market Forecast - By Region 2.27
Graph 2.53: Enterprise Security Market Forecast - By Region 2.27
Graph 2.54: Enterprise Security Market Forecast - North America 2.28
Graph 2.55: Enterprise Security Market Forecast - EMEA 2.28
Graph 2.56: Enterprise Security Market Forecast - Central and South America 2.28
Graph 2.57: Enterprise Security Market Forecast - Asia Pacific 2.29
Graph 2.58: Enterprise Security Market Forecast - EU 2.29
Graph 2.59: Enterprise Security Market Forecast - US 2.29

Charts, Tables & Graphs—Part TWO

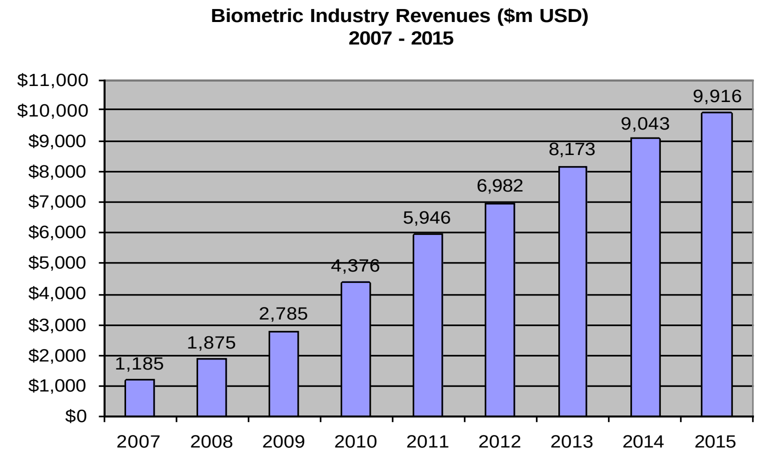
Table 2.22: Financial Services Market Forecast - Global, EU, US 2.30
Graph 2.60: Financial Services Forecast - Global, EU, US 2.30
Table 2.23: Transportation Market Forecast - Global, EU, US 2.30
Graph 2.61: Transportation Market Forecast - Global, EU, US 2.30
Table 2.24: Information Transactions Market Forecast - Global 2.31
Graph 2.62: Information Transactions Market Forecast - Global 2.31
Table 2.25: Information Transactions Market Forecast - By Region 2.31
Graph 2.63: Information Transactions Market Forecast - By Region 2.31
Graph 2.64: Information Transactions Market Forecast - North America 2.32
Graph 2.65: Information Transactions Market Forecast - EMEA 2.32
Graph 2.66: Information Transactions Market Forecast - Central and South America 2.32
Graph 2.67: Information Transactions Market Forecast - Asia Pacific 2.33
Graph 2.68: Information Transactions Market Forecast - EU 2.33
Graph 2.69: Information Transactions Market Forecast - US 2.33
Table 2.26: Healthcare Market Forecast - Global, EU, US 2.34
Graph 2.70 Healthcare Market Forecast - Global, EU, US 2.34
Table 2.27: Financial Services Market Forecast - Global, EU, US 2.34
Graph 2.71: Financial Services Market Forecast - Global, EU, US 2.34
Table 2.28: Financial Transactions Market Forecast - Global 2.35
Graph 2.72: Financial Transactions Market Forecast - Global 2.35
Table 2.29: Financial Transactions Market Forecast - By Region 2.35
Graph 2.73: Financial Transactions Market Forecast - By Region 2.35
Graph 2.74: Financial Transactions Market Forecast - North America 2.36
Graph 2.75: Financial Transactions Market Forecast - EMEA 2.36
Graph 2.76: Financial Transactions Market Forecast - Central and South America 2.36
Graph 2.77: Financial Transactions Market Forecast - Asia Pacific 2.37
Graph 2.78: Financial Transactions Market Forecast - EU 2.37
Graph 2.79: Financial Transactions Market Forecast - US 2.37
Table 2.30: Consumer Market Forecast - Global, EU, US 2.38
Graph 2.80: Consumer Forecast Market - Global, EU, US 2.38
Table 2.31: Interbank Services Market Forecast - Global, EU, US 2.38
Graph 2.81: Interbank Services Market Forecast - Global, EU, US 2.38
Table 2.32: North America Key Public Sector Market Forecast 2.39
Graph 2.82: North America Key Public Sector Market Forecast 2.39
Table 2.33: North America Key Commercial Market Forecast 2.39
Graph 2.83: North America Key Commercial Market Forecast 2.39
Table 2.34: EMEA Key Public Sector Market Forecast 2.40
Graph 2.84: EMEA Key Public Sector Market Forecast 2.40
Table 2.35: EMEA Key Commercial Market Forecast 2.40
Graph 2.85: EMEA Key Commercial Market Forecast 2.40
Table 2.36: South and Central America Key Public Sector Market Forecast 2.41
Graph 2.86: South and Central America Key Public Sector Market Forecast 2.41
Table 2.37: South and Central America Key Commercial Market Forecast 2.41
Graph 2.87: South and Central America Key Commercial Market Forecast 2.41
Table 2.38: Asia Pacific Key Public Sector Market Forecast 2.42
Graph 2.88: Asia Pacific Key Public Sector Market Forecast 2.42
Table 2.39: Asia Pacific Key Commercial Market Forecast 2.42
Graph 2.89: Asia Pacific Key Commercial Market Forecast 2.42

Executive Summary

The biometrics industry will experience significant transformation over the next ten to fifteen 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 transaction based.

The good news is that these dynamics will create an environment conducive to the level of market expansion needed to realize the promise of biometrics. The not so good news is that as growth continues and potential rewards increase so to will uncertainty and risk. Successful navigation of this market transformation will require a clear strategic vision of the inevitable future of the industry and the resources to exploit the opportunity gaps created by a market in flux.

Biometrics Industry Revenues 2007—2015



©Acuity Market Intelligence 2007

Graph 1.1

Market Growth

The market for biometrics technology is poised for sustained growth with global revenues approaching nearly $10 billion annually by 2015. This growth will be driven by broad *Mega Trends* impacting global IT development as well by solutions *Meta Drivers* within specific application areas. Mega and Meta influences lead to the inevitability of biometrics and create a context for understanding the likely evolution of the marketplace and the associated strategic opportunities.

Mega Trends

Seven global *Mega Trends* will profoundly impact all IT development through 2020 and have important, specific implications for biometrics. They are:

- Globalization and Third World Development
- 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

Each of these trends impacts and is impacted by the management and linking of large populations to identity based rights, privileges, actions, and services. The sheer volume and complexity of dealing with individual identification in a global community that is simultaneously shrinking (ever more connected) and expanding (ever more inclusive) is staggering.   In this environment, the ability to establish and link an individual to an established or claimed identity is fundamental to creating and maintaining the digital infrastructure on which the global community increasingly relies.

Meta Drivers

Application Solution *Meta Drivers* shape the opportunities for widespread deployment of biometrics. Technology Evolution *Meta Drivers* are the capabilities that support the demands of these market forces.

The three key Public Sector *Application Solution Meta Drivers* are: eBorders, eID, and eGovernment. The most immediate drivers are worldwide government mandates for integrated border management systems. This includes the development of biometrically enabled travel documents and the devices and border control systems that utilize them, expedited passenger programs, transportation worker identification and access control systems and immigration and asylum seekers application, identification and monitoring systems. Government endorsement of biometrics for these applications has already begun to produce standards and create an environment where interoperable, large-scale systems are now transitioning from vision to practical reality. This endorsement also has begun to drive wide spread government adoption of biometric authentication for government electronic identification programs and will ultimately lead to the adoption of biometrics for secure, fully transactional eGovernment capabilities.

The three key Commercial *Application Solution Meta* Drivers are: Enterprise Security, Information Transactions, and Financial Transactions. The Commercial market has benefited by the current drive towards large-scale interoperable systems for government applications. The rampant growth of identity theft and associated requirements for the protection and management of personal data will contribute significantly to growth in this area as well. Adoption in the enterprise market for physical and logical access is beginning to occur and will gain significant market traction over the next three years. This will be rapidly superseded by the much larger opportunity to secure information and financial transactions which will emerge over the next five to ten years.

The four key *Technology Evolution Meta Drivers* are: Secure Identity Core, Secure Credentials, Secure Transaction, and Secure Mobility. These capabilities are essential components of the larger framework enabling the development of a reliable, secure, worldwide infrastructure that biometric authentication simultaneously plays a central role in creating and relies on for market expansion

Solution Adoption Framework
One of the most important factors to consider when evaluating the evolution of the biometrics industry is the development of the marketplace relative to adoption lifecycles (based on the work of Geoffrey Moore, author of *Crossing the Chasm)*. The Solutions Adoption Framework illustrates the relationship between the evolution of the biometrics core technology adoption lifecycle and the evolution of the biometrically enabled solutions adoption lifecycle. This framework indicates that the current state of the market for biometrics technology is moving rapidly into the "Main Street" or mainstream realm, while solutions development is still in the "Early Markets" phase. Essentially, the technology is ready for mainstream adoption but the solutions are still immature.

Solutions Adoption Framework

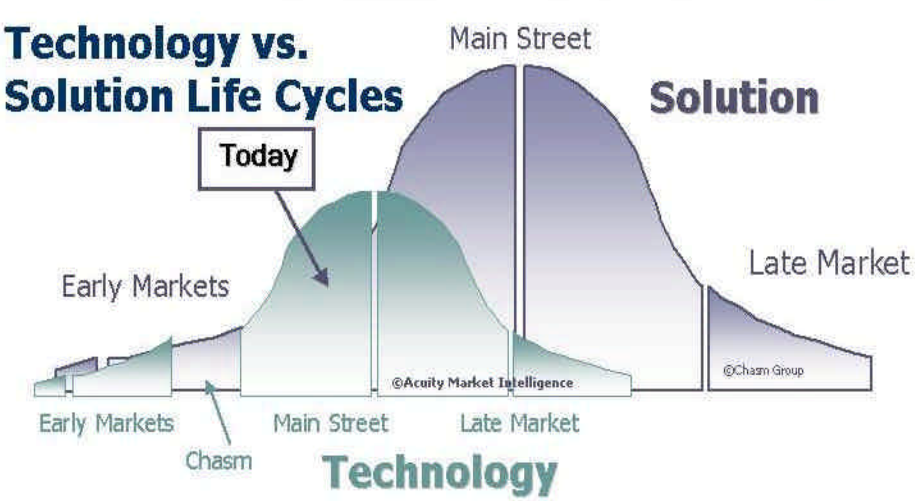


Chart 1.1

Obstacles and Opportunities
Mainstream biometric deployment faces obstacles ranging from inherent limitations of the technology and failure to adequately plan for and implement deployments to fears about violations of privacy and civil liberties. These obstacles are primarily related to moving biometrics deployments from relatively small, close loop technology-centric applications to large scale human-centric identification solutions. This requires the development of a secure standards based technology infrastructure, a privacy respecting if not enhancing legal and regulatory framework, and human factors based system design that paves the way for truly interoperable, user accessible, and socially acceptable solutions. One of the more intriguing aspects of the marketplace is that many of these real and perceived obstacles represent significant opportunities for biometrics market development as well. The most effective strategic response is to transform obstacles into opportunities through the appropriate use of biometrics.

Four key areas of concern considered outside the purview of biometrics, nonetheless critical to the mainstreaming of biometrics, reflect this phenomenon. They are: Privacy, Centralized Databases, Single View of Identity, and Identity Theft/ Fraud. Proactive engagement by market players can ensure that biometrics enhance rather than threaten consumer and citizens within each of area of concern.

There are also issues central to deploying biometrics where obstacles and opportunities are integrally linked. Two categories of concern are Bridging the Human-Machine Identity Gap and Solutions Development. Bridging the Human-Machine Identity Gap recognizes that the complexity of developing and implementing biometrics rests in the nature of the technology, that is, in the fact that biometrics is a science of human/machine interaction. Three aspects of this divide warrant distinction: Enrolment, Human Factors, and Privacy. Historically, Solutions Development has received minimal attention within he biometrics industry relative to the almost exclusively focus on the performance and reliability of the technology. This is typical of any emerging technology market and has not yet posed a hindrance to the overall evolution of the marketplace. However, in order for biometrics to enable broad-based identification solutions, the technology must be developed and integrated within a larger solutions context. Four components crucial to this process are: Extensible Security, Context Specific Identity, Price/Performance, and Interoperability.

Future for Key Technologies

Mainstream ubiquity will occur as capture devices for most routine applications will become cheap, reliable commodities available in multiple form factors embedded in everything from PDAs, PCs, POS terminals, and ATMS to vehicles, security gates and appliances. As with most technology, these devices will blend into the landscape of modern life and become essentially invisible. Do you know who makes the hard drive in your PC? How the bank processes your pin number at an ATM? Convenience will rule and except for high security applications or high value transactions, where more specialized equipment may be required, biometrics will become utterly mundane and the technology to process them virtually interchangeable. Selection of modalities will be based on the circumstances of any given solution.

In the more distant future—beyond the timeframe of this report—the actual distinctions between biometrics modalities will blur, massive convergence will take hold, and individual biometric categories will disappear. This is more than just one technology winning out over another but an actual merging and morphing of the capture devices and the algorithms. Ultimately, capture devices and algorithms will to be mostly indifferent, regardless of scale, to the nature of the type of pattern-data being captured.

Most biometric will continue to improve in performance and accuracy until their maximum capability has been achieved. Others, such as hand recognition, may simply fade away as their price/performance and usability as compared to other modalities no longer makes them viable.

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 Confirmation and Surveillance—to create market segmentation matrices. This segmentation 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.

Public Sector

The *Public Sector Market Segmentation Chart* (below) defines the specific markets that provide the most significant opportunities for biometrics solutions within the three sub domains of 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 – which includes national and other identity cards, benefits distribution, voter registration, drivers licenses, and 3) eGovernment – fully transactional interactive service delivery for citizens and commercial enterprises. Similarly, the specific markets within each sub domain selected for this segmentation represent areas of most probable and significant growth for biometrically enabled solutions over the analysis period. not the complete opportunity within that given sub domain.

Public Sector Market Segmentation

* Solutions for these markets will likely be paid in part by commercial enterprises		Integrated eBorders				eID				eGovernment	
		Travel Docs	*Port Facilities	*Vehicles	*Expedited Travelers	Civil - DL, National, Voter	Benefits - Health, Welfare	Government Admin - Civil Servants	Military & Defense - Staff & Contractors	Citizen - Tax, License, Utilities, Court, Education	Commercial - Tax, License, Regulatory, Court
Physical Access – Facility Access, Security Checkpoints	Citizens		X	X	X						
	Staff & 3rd Parties	X	X	X	X	X	X	X	X		
Logical Access – PC, Networks, Mobile Devices, Kiosks	Citizens	X	X		X	X	X			X	X
	Staff & 3rd Parties	X	X	X	X	X	X	X	X	X	X
Identity Services – Background Check, Document Issuance, Enrollment	Citizens	X	X		X	X	X			X	X
	Staff & 3rd Parties	X	X	X	X	X	X	X	X	X	X
Surveillance & Detection – Cooperative & Non-cooperative including watchlists	Citizens		X	X	X					X	X
	Staff & 3rd Parties	X	X	X	X	X	X	X	X	X	X

Chart 1.2

Commercial Market Segmentation

		Enterprise Security			Information Transactions				Financial Transactions			
		Financial Service	Healthcare	Transportation	IP Management	Travel	Financial	Health	Consumer	B2B	ATM	Inter-bank Transfer
Physical Access – Facility, Access, Secure Area Access	Customers			X								
	Staff & 3rd Parties	X	X	X							X	
Logical Access – PC, Networks, Mobile Devices, Kiosks, Accounts, IP	Customers	X	X	X	X	X	X	X	X	X	X	X
	Staff & 3rd Parties	X	X	X	X	X	X	X	X	X	X	X
Identity Services – Background Check, Document Issuance, Enrollment	Customers	X	X	X	X	X	X	X	X	X	X	X
	Staff & 3rd Parties	X	X	X	X	X	X	X	X	X	X	X
Surveillance & Monitoring – Cooperative & Non-cooperative including Time & Attendance and Watchlists	Customers	X	X	X	X	X	X	X	X	X	X	X
	Staff & 3rd Parties	X	X	X	X	X	X	X	X	X	X	X

Chart 1.3

Commercial

The Commercial *Market Segmentation Chart* (above) defines the specific markets that provide the most significant opportunities for biometrics solutions within the three sub domains of 1) Enterprise Security - which includes physical and logical access for employees and third parties (customers, vendors, etc.) as well as credentialing and surveillance, 2) Information Transactions – corporate and personal access to travel, financial and healthcare information as well as IP management for technical, scientific and research firms, and 3) Financial Transactions – consumer, business to business, ATM and inter-bank transactions. Similarly, the specific markets within each sub domain selected for this segmentation represent areas of most probable and significant growth for biometrically enabled solutions over the analysis period. not the complete opportunity within that given sub domain.

Major Research Findings

Over the next 10 years the infrastructure to enable mainstream, ubiquitous biometric authentication will be developed. Biometrics will be a critical 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.

Key Forecasts

- Commercial deployment revenues will begin to supersede Public Sector revenues in 2012 and will represent more than 52% of the total global market for biometrics core technology by 2015.
- 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). By 2014, the Asia Pacific Region will generate the greatest revenues for the biometrics industry.
- Transactions will ultimately provide the majority of industry revenue. Information and financial transactions for Commercial applications by 2012 and eGoverment for Public Sector applications by 2015.

Biometrics Industry Market Share: Public Sector vs. Commercial 2007 and 2015

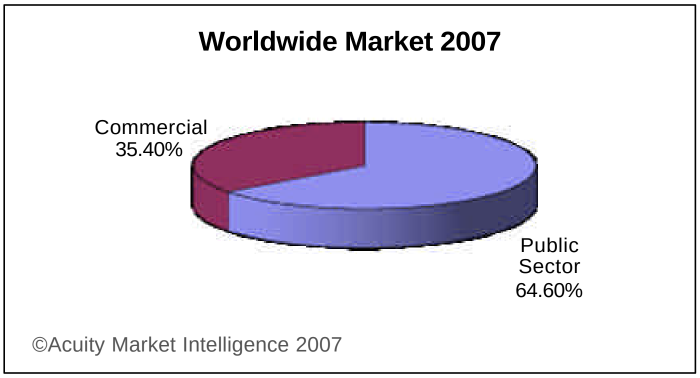


Chart 1.4

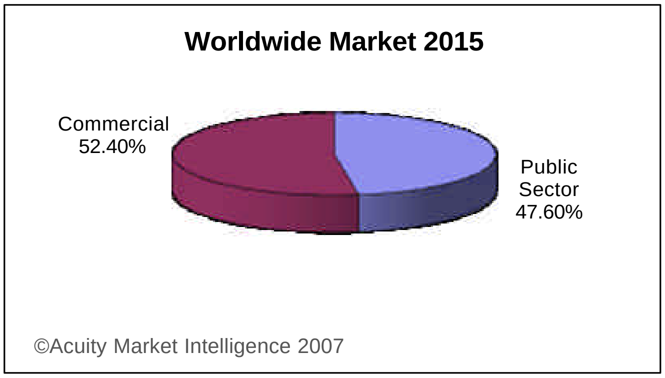
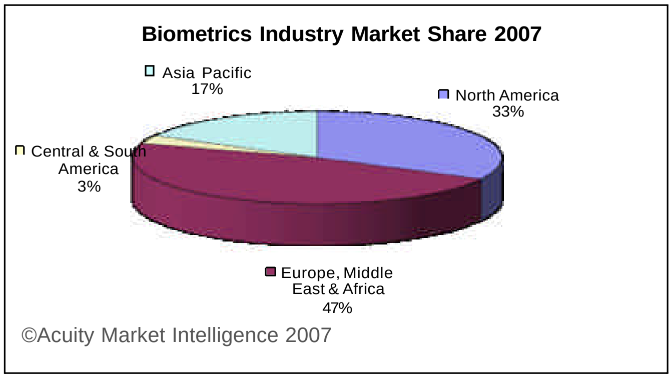


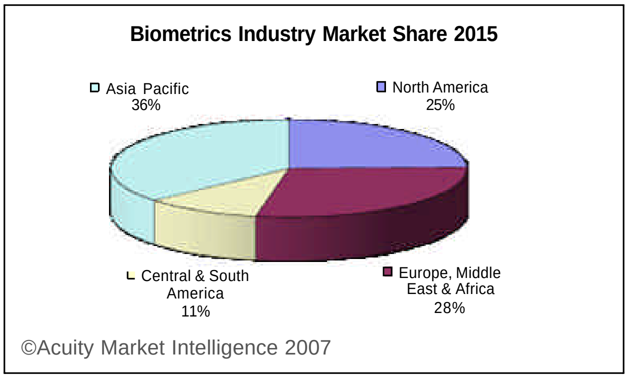
Chart 1.5

Market Share by Region 2007 and 2015



©Acuity Market Intelligence 2007

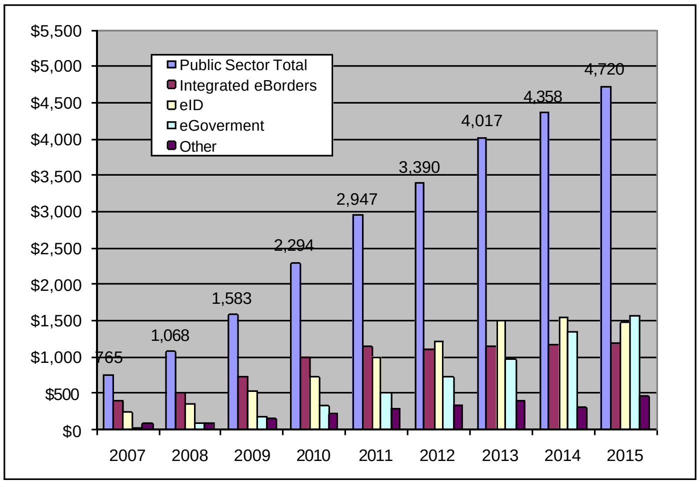
Chart 1.6



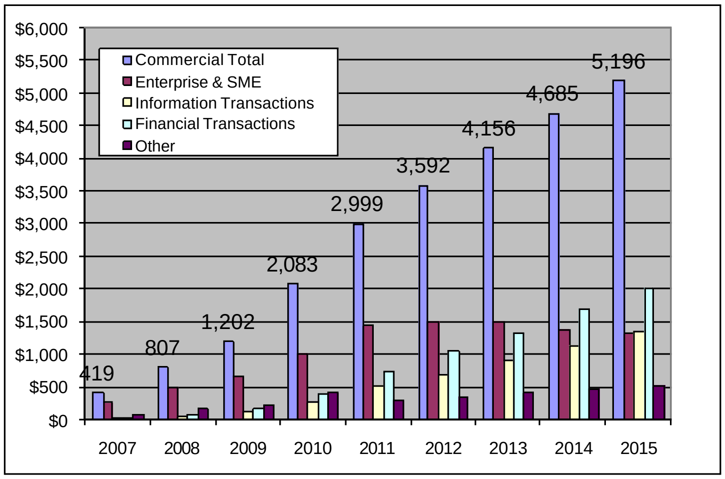
©Acuity Market Intelligence 2007

Chart 1.7

Public Sector and Commercial Revenue 2007—2015



Graph 1.2



Graph 1.3

Key Analysis Findings:

- A confluence of factors including the emerging central role of the Digital Identity in IT, population mobility and workforce decentralization, demand for eGovernment services, near ubiquitous reliance on digital transactions, and the inevitability of broadband access everywhere will require a level of authentication available only through the use of biometrics.

- The entry of sophisticated, well funded market players with technology expertise in high resolution image capture, large scale data management and high speed processing, and pattern recognition and matching algorithms from varied fields such as robotics, astronomy, and intelligent video elevate technological capability and provide the requisite knowledge for the industry to experience sustained growth.

- Contactless, user acquiring biometrics will become a preferred method of authentication for two primary reasons. Capture technology will become increasingly more sophisticated operating accurately regardless of environmental conditions. Biometric authentication that does not require the user to "do anything" e.g. position themselves in relation to or have physical contact with a reader, will be prove safer (no transmission of germs) and more convenient for users.

- Secure transaction capability will ultimately define the genuine opportunity for large scale, wide spread deployment of biometric technologies. The technology itself will, in many respects, become inconsequential as the applications it delvers become essential components of 21st century life.