


VIII ATLANTIC SYMPOSIUM ON C4I



## Identity and Authentication Management Systems for Access Control Security

INTELLIGENCE  
In Global Age

AFCEA PORTUGAL

Lisbon, May, 9th, 2007 Capitulo 226

Good Afternoon!

Since Yesterday we have been talking about threats and how to deal with those threats in order to protect ourselves from individuals and protect people, information, buildings, countries and organizations.

The discussion has been:

What and which profile is behind from these threats?

How can we reduce and minimize the risks from those threats?

How can we prevent those threats and be proactive in our actions?

How is technology dealing with those threats?

How can we take advantage from technology to reduce risks?

The world has changed!

Since the end of the cold war the menaces know come from different directions and from knew ways.

Globalization in its all dimensions (cultural, financial, trade, information) is unbalancing our lifes.

My presentation is the outcome, at this moment, of our experience on field projects regarding the usage of technology and information systems to enhance Security

# Global Challenges

## Globalization

- Cultural
- Financial
- Trade
- Information
- ....

## Terrorism

Enable Information Sharing Across Boundaries

Protection of Infrastructures

Mass Migration Flows

Provide better service to citizens



I think there is no doubt in this room the world has changed!

The globalization has narrowed the world but also brought along with it new challenges and new threats creating a world with different speeds of economical and cultural development.

Today information can be accessed from any part of the world, from anybody at any place our breaking down walls and overcome borders.

The threats against countries sovereignty and its people are coming today from terrorism and the challenge is how to prevent such actions.

Terrorism as put us another challenge: a challenge of cooperation enabling Information and sharing it across country boundaries.

The different regional economical development speeds created mass migrations flows of people looking for new opportunities, and sometimes for an opportunity of survival.

Citizens are looking for better services from its Governments there is new challenge to improving Public Administration.

VIII ATLANTIC SYMPOSIUM ON C4I

## Global Answers

- Electronic Passports
- National Identity Cards
- Centralized Biometric Data Bases
- Centralized Event Data Bases
- Government intelligence and law Enforcement information interoperability
- World globalization implies more people mobility and a need for more VISA Control
- Implementation of Frequent Travel Programs
- Automatic document authentication for secure borders ("watch lists")
- Monitoring, record and mass migration flows
- More Efficiency, Effectiveness in CITIZEN AUTHENTICATION

**Real Time Identity Verification Document Authentication**

**Centralized Biometric Data Bases**

**Interoperability Between agencies and institutions**

**Efficiency, Effectiveness in Identity Verification and Documental Authentication**

**Increase Security, Reduce Threats, Minimize Risk**

**AFIS Automated Fingertip Identification System**

**SINFIC**  
Resposta, Agilidade e Qualidade em Tecnologias de Informação

Regarding these challenges there are already some answers:

The Electronic Passports to control monitor univocally each person in mass migration and visa issuing

National Identity Cards to provide a better service from Governments to citizens

Centralized Biometric Data Bases and Centralized Event Data Bases for sharing information across countries and agencies to increase countries security

Government intelligence and law Enforcement information interoperability to analyze patterns of behavior

World globalization implies more people mobility and a need for more VISA Control

Implementation of Frequent Travel Programs to credentialing good citizens

Automatic document authentication for secure borders ("watch lists") to prevent identification fraud

Monitoring, record and mass migration flows for security reason

More Efficiency, Effectiveness in CITIZEN AUTHENTICATION making sure that you are who you claim to be

VIII ATLANTIC SYMPOSIUM ON C4I

**BIO MS**  
Bioscience & Information Management Systems

**WHAT IS THE REAL PROBLEM?**



**SINFIC**  
Instituto de Informática e Estatística em  
Tecnologias de Informação

What is behind? What problem are we trying to solve?

## World Questions



- Should I grant this individual with a credential?
- Has for this individual already been issued a credential?
- Is this person authorized to access the information?
- Is this person authorized to access the building
- Is this person authorized to access to this service?
- Has this person the privilege to access these citizen rights?



If we take a look at the challenges we have been trying to answer these questions arise:

Should I grant this individual with a credential?

With National ID card? Is he trustful?

Has for this individual already been issued a credential?

Is he faking multiple Identities?

Is this person authorized to access the information?

How are we verifying its identity and authenticate is documents?

Is this person authorized to access the building? Is this person authorized to access to this service? Has this person the privilege to access this citizen rights?

Is he in a “watch list” database? And has granted authorizations and access privileges?

## How Do I know Who You Are?

Did You Know :

- The nineteen 9/11 hijackers had a total of 63 valid driver licenses
- There are approximately 5 million identity thefts yearly in US
- 7 million victims of credit card fraud only in US
- People do not protect their credentials

Methods based on credentials, passwords and Identities based on external reference number are not currently adequate.



Another question crucial question is: How Do I know Who You Are? Or do you claim to be?

Did You Know :

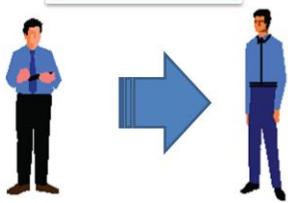
- The nineteen, 9/11 hijackers had a total of 63 valid driver licenses
- There are approximately 5 million identity thefts yearly in US
- There are 7 million victims of credit card fraud only in US
- People do not protect their credentials

The Conclusion is: Methods based on credentials (ID documents), passwords and Identities based on external reference number is not currently adequated anymore!

VIII ATLANTIC SYMPOSIUM ON C4I


**Types Identification Fraud**

**Changing Identity**

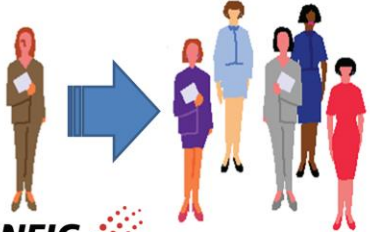


**How?**

Assume someone else's Identity




**Faking Multiple Identities**



**How?**

Issuing Several Documents



**SINFIC**  
 Especial, Agilidade e Qualidade em  
 Tecnologias de Informação

**BIO MS**  
 Biometric Identification & Access Control System

As we have seen there are 2 different types of ID fraud:

Changing identity, assuming other persons' identity forging and using credential as their own such as: passport, id card, drivers license (like the 9/11 hijackers), military card, property registration...

Or

Faking multiples identities changing their look and producing different cards for several different names

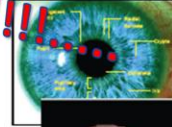
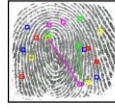
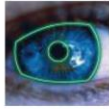
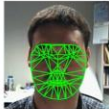
# Biometric Recognition



• Personal recognition based on:

- Who you are
- What you Know (PIN Card)
- What you have (ID Card)

**IS NOT ENOUGH !!!!!**



• We need a more powerful tool: Biometrics!

- Biometric Recognition - recognition of a person by his own characteristics and then link that body to an external trustful established identity
- Biometric Credentialing – documents with univocally identifiable, i.e., documents linked to the individual unique characteristics (biometric)



We have seen that Personal recognition based on Who you are; What you Know (PIN Card), What you have (ID Card) it is simply not enough!

We have to search for other answers adding technology to Personal Recognition

We need a more powerful tool: Biometrics! Combined and mixed with Personal Recognition model.


We need:

Biometric Recognition – which is the recognition of a person by his own characteristics and linked that body and to an external trustful established identity

We need also,

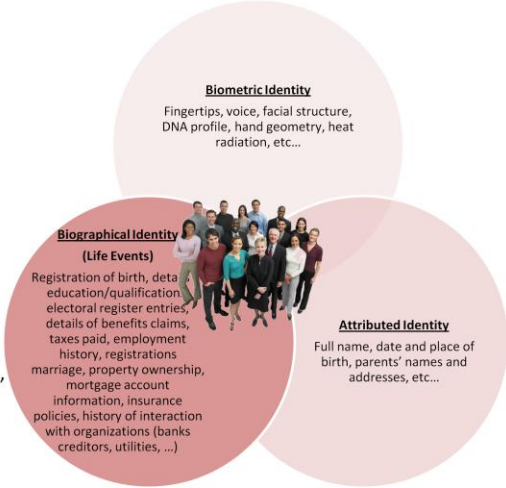
Biometric Credentialing – which are documents linked to a unique individual through its own characteristics (biometric)

VIII ATLANTIC SYMPOSIUM ON C4I

 **BIO MS**  
Biosensing & Authentication Research Group

## 3 Elements of Identity


- Biometric Identity –
  - Attributes that are unique to an individual
- Identity Attributes –
  - Components of a person that are given at birth
- Biographical Identity –
  - Build up of the identity over time, life events that cover how an identity, a person interacts with the society



**Biometric Identity**  
Fingertips, voice, facial structure, DNA profile, hand geometry, heat radiation, etc...

**Biographical Identity (Life Events)**  
Registration of birth, details of education/qualification, electoral register entries, details of benefits claims, taxes paid, employment history, registrations marriage, property ownership, mortgage account information, insurance policies, history of interaction with organizations (banks, creditors, utilities, ...)

**Attributed Identity**  
Full name, date and place of birth, parents' names and addresses, etc...

 **SINFIC**  
Instituto de Engenharia e Tecnologia de Informação

But a good Identity Management System has to deal with the 3 elements of Identity:

**Biometric Identity – Attributes that are unique to an individual**

Examples; Fingertips, voice, facial structure, DNA profile, hand geometry, heat radiation, etc...

**Identity Attributes – Components of a person that are given at birth and remain unchanged during lifetime**

Examples; Full name, date and place of birth, parents' names and addresses, etc...

**Biographical Identity – Are life events of a person interaction with the society**

Examples; Registration of birth, details of education/qualifications, electoral register entries, details of benefits claims, taxes paid, employment history, registrations marriage, property ownership, mortgage account information, insurance policies, history of interaction with organizations (banks, creditors, utilities, ...)

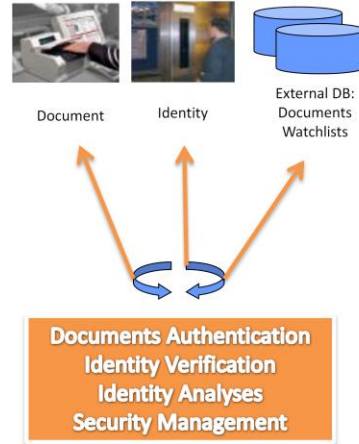
## Identity Challenges

### Challenges

- Is the applicant presenting “authentic” documents?
- Does the document belong to the applicant?
- Real Time identity verification with external party databases?

### Solutions

- Enable officers to check and file proofing documents
- Verify if applicants exist in the database
- Verify identity biometric features
- Ensure accurate data collection at the front end



The front end identity challenges are:

Is the applicant presenting “authentic” documents?

Does the document belong to the applicant?

Real Time identity verification with external party databases?

And the Solutions are:

Enabling officers to check and file proofing documents

Verifying if applicants exist in the database

Verifying identity biometric features

Ensuring accurate data collection at the front end

VIII ATLANTIC SYMPOSIUM ON C4I

# Identity Management System Requirements

**BIO MS**  
Biometric Identity & Access Management System

- Establishing a trusted identity
- Prevent document fraud
- Easy identity verification
- Establishing a reliable identity authentication
- Provide convenient access to services
- Prevent misuse
- Reduce identity management costs
- Avoid identity theft

**One Person  
One Identity  
One Document**

**AFIS**  
Automated Fingerprint Identification System

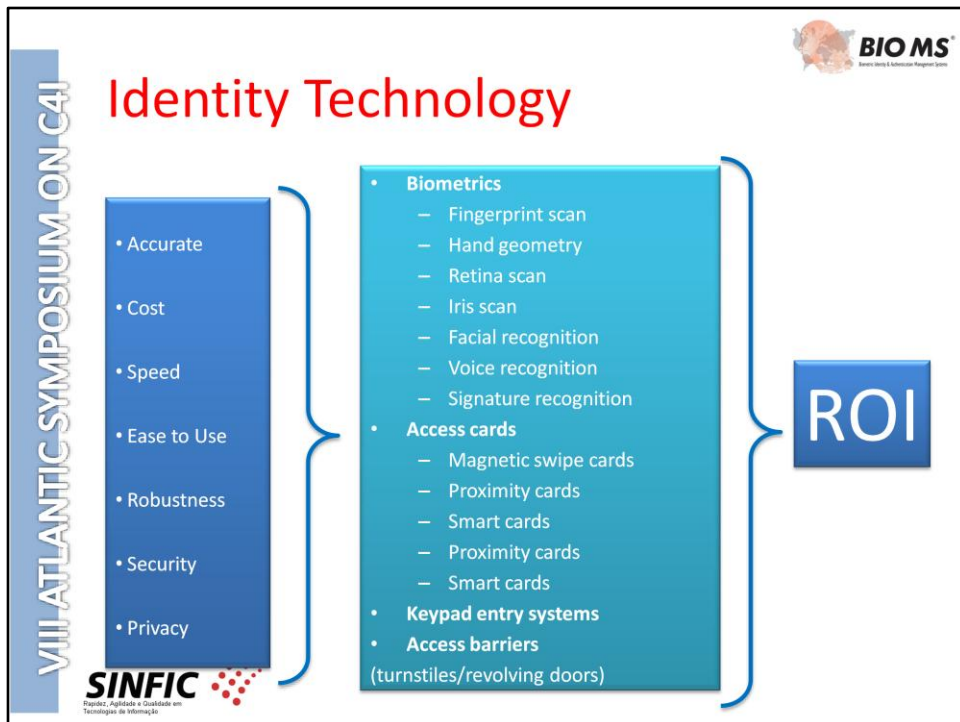
**ABIS**  
Automated Biometric Identification System

**SINFIC**  
Esperto, Ágilidade e Qualidade em Tecnologias de Informação

The requirements for an Identity Management Systems are to manage in a integrated way the:

- Establishing of a trusted identity
- Prevention of document fraud
- Easy identity verification
- Establishing a reliable identity authentication
- Provide convenient access to services
- Prevent misuse
- Reduce identity management costs
- Avoid identity theft

To manage all this we have to have an AFIS - Automatic Fingertip Identification System and ABIS - Automatic Biometric Identification System as the backbone of an IDMS



There are several technologies available in the market

Biometric

Access Cards

Keypads

Access Barriers

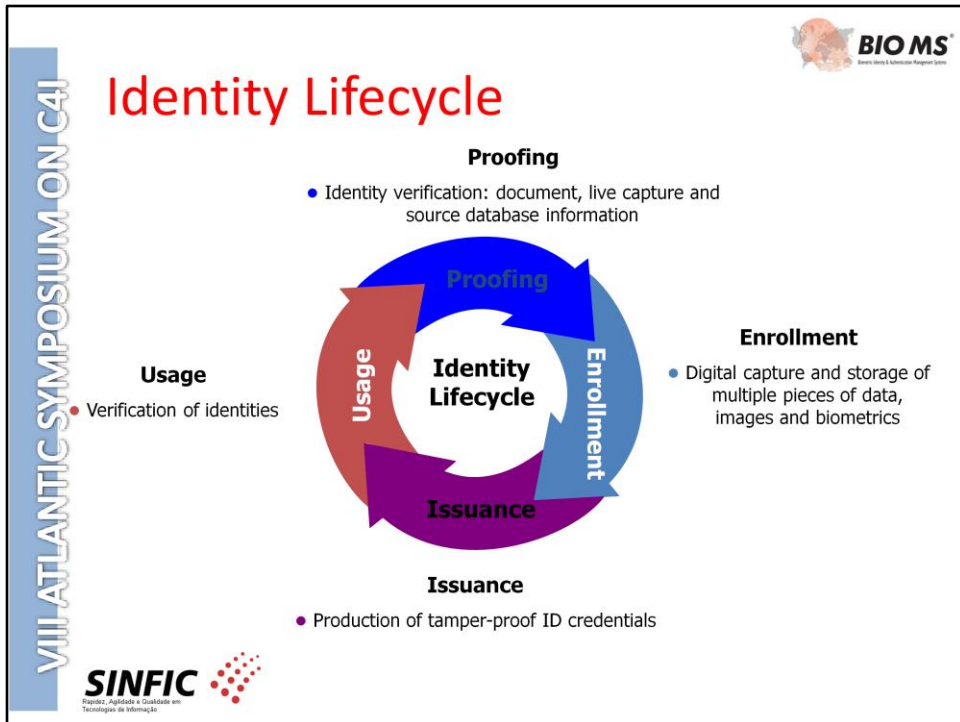
The good system is the combination of these tech that make an ID Authentication Management System

The answer is a solution that manages the ID's complete life cycle

The biometry is the identity technology used in these days.

And a good IDMS has to connect and link to several and different biometric technologies in order to create a "strong" identity for any individual...for authentication and verification purposes.

... and of course, costs matter... there is biometric technology more costly than other...for example, the iris is more expensive (for the moment), more enduring and more accurate than fingertips...



And good IDMS has also to manage the identity life cycle:

**Proofing** Identity verification: where document are live capture and the information read sourced in a external database

**Enrollment** : Is the collection and digital capture and storage of multiple pieces of biometrics data

**Issuance**: Is the phase of production ID credentials

**Usage**: Is the ID verification using e ways of biometric authentication or through credentialing (like e-passports)

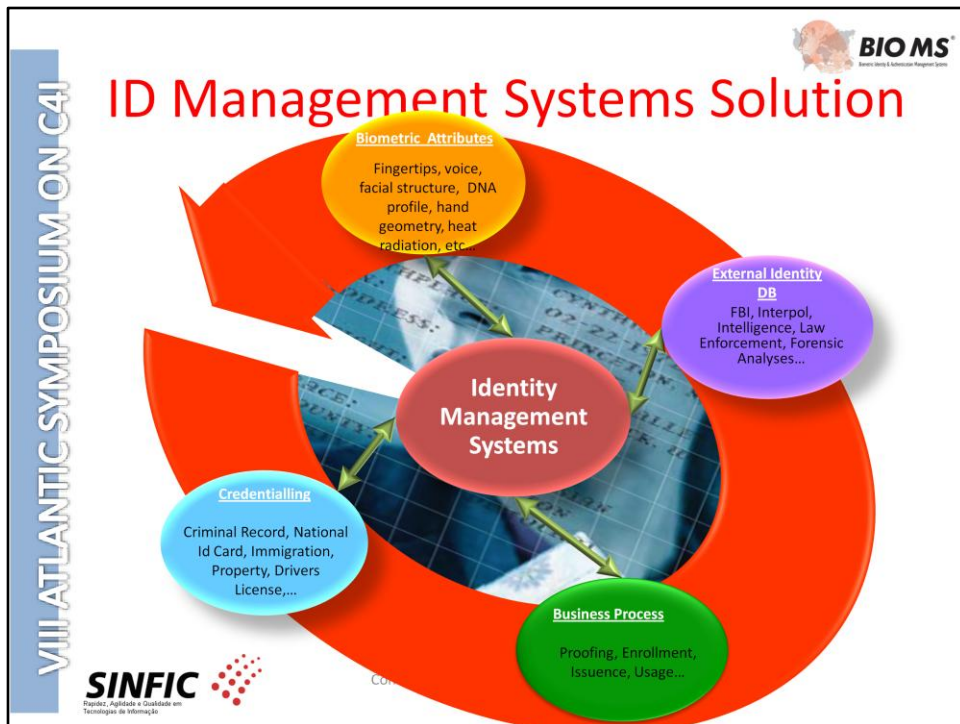
VIII ATLANTIC SYMPOSIUM ON C4I

**BIO MS**  
Biosensors & Information Management Systems

**HOW CAN TODAY TECHNOLOGY HELP?**

**SINFIC**  
Esperteza, Agilidade e Qualidade em  
Tecnologias de Informação

We have seen that biometric technology as the ability to help?  
But how can we use it in a integrated way that we may to manage identity?



The Identity Management Systems have to integrate and manage:

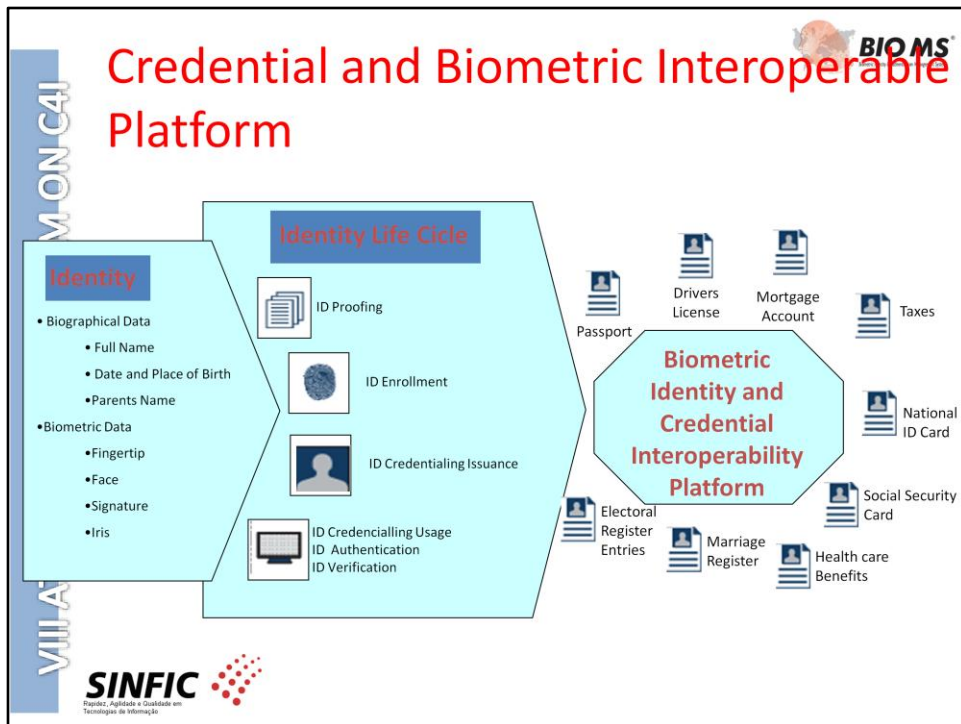
Biometric Attributes – to create a unique identity

Credentialing – for producing authenticate documents

Business Process - to manage the identity lifecycle and customer requirements

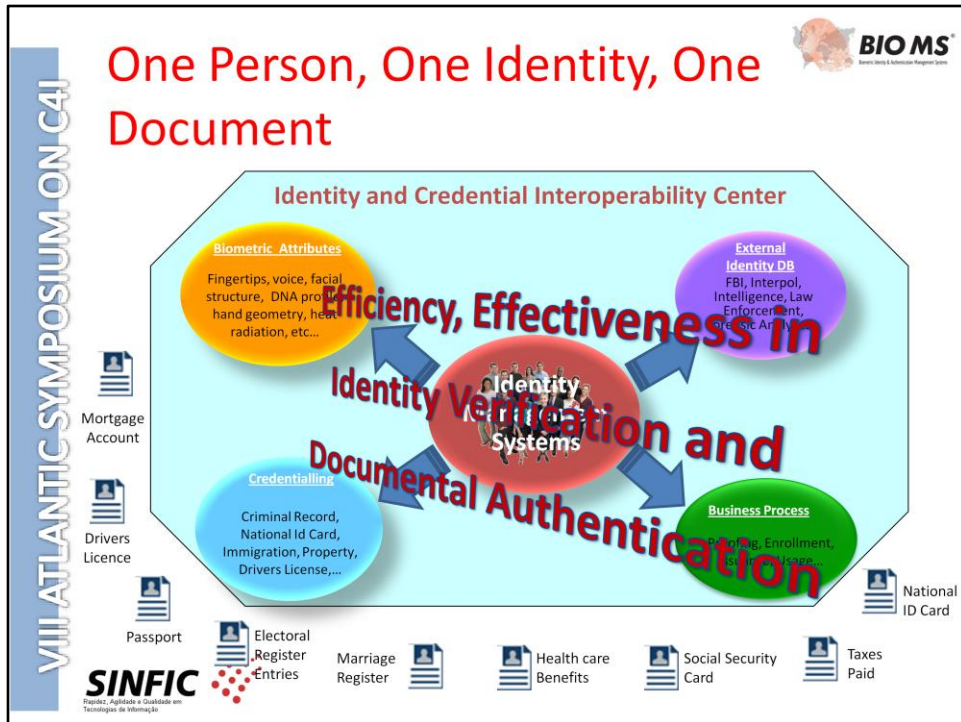
External Identity DB – for sharing information with other organizations

A thus we have a system that is suitable for any market requirements and purposes.



The Identity Management Systems are also build in Interoperable Biometric Platform that allows to manage:

- Several biometric technologies independently
- Different types Identity verification and document authentication
- Produce and manage several credentials for different purposes



This way IDMS can:

Reduce Implementation and development COSTS

Choose the best and most suitable biometric technology for a certain purpose and also to combine it into an identity

Be more Efficient, Effective in Identity Verification and Documental Authentication

## Summary

- Biometric Technology is not the panacea for the global threats
- Technology Cannot Compensate for Human Failure or Ineffective Security Processes
- The Capabilities of Security Technologies Can Be Overestimated
- The Use of Several Security Technologies Continues to Generate Concerns about their Potential Violation of Expectations of Privacy



Biometric Technology is not the panacea for the global threats as we have learned from past experiences...but can help us reducing fraud and increasing access security  
 Technology Cannot Compensate for Human Failure or Ineffective Security Processes  
 The Capabilities of Security Technologies Can Be Overestimated  
 The Use of Several Security Technologies Continues to Generate Concerns about their Potential Violation of Expectations of Privacy...but we still have to balance between what we want to protect and our privacy

# Summary

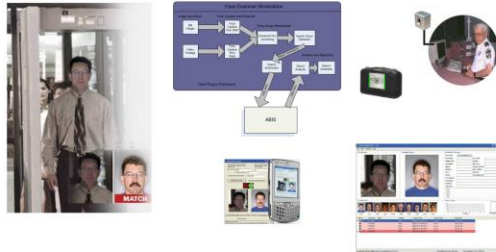


An Identity Management Systems has to be able to manage the 3 elements of the ID:

- Biometric Identity
- Identity Attributes
- Biographical Identity (Events)

... and also able to manage:

- The identity lifecycle
- Linked to external databases
- Usage of access cards
- Connected to access "barriers"
- Video streaming from surveillance cameras



An Identity Management Systems has to be able to manage the 3 elements of the ID:

- Biometric Identity
- Identity Attributes
- Biographical Identity (Events)

... and also able to manage:

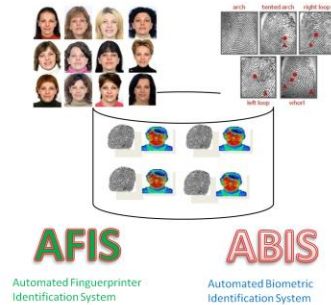
- The identity lifecycle
- Linked to external databases
- Usage of credentials
- Connected to access "barriers"
- Video streaming from surveillance cameras

## Summary

Identity Management Systems have algorithms

for Identity:

- Biometric data quality control
- Real-time searches
- Duplicate analyses



Biometric data quality control to provide the usage and interoperability to other departments or external users

Real-time searches with good performances for identity verification, for example law enforcements and building security

Duplicate analyses

Identity Management Systems have to have algorithms for Identity:

Biometric data quality control

Real-time searches

Duplicate analyses

## Summary

- Identity Management Systems Can Enhance Security:
  - Enabling information sharing
    - Database Integration among agencies and organizations
      - Law Enforcement
      - Intelligence Agencies
      - Border Crossing
      - Homeland Departments
  - Provide Intelligence to counter terrorism
  - Monitoring mass migration flows
  - Identity Management Systems gives answers to the questions:
    - Who are you?
    - Where you able to go?
    - What are you entitled to do?



**Are You Who You  
Claim To Be?**

**“For terrorists, travel documents are as important as weapons”**

**Source: 9/11 Commission Report**

**SINFIC**  
 Segurança, Agilidade e Qualidade em  
 Tecnologias de Informação

### Identity Management Systems Can Enhance Security:

Enabling information sharing

Database Integration among agencies and organizations

Law Enforcement

Intelligence Agencies

Border Crossing

Homeland Departments

Provide Intelligence to counter terrorism

Monitoring mass migration flows

Identity Management Systems gives answers to the questions:

Who are you?

Where you able to go?

What are you entitled to do?

Or Are You Who You Claim To Be?

Finally

I only would like to mention that this work is based on our field experience in IDMS project , where we are building and developing a database with 50 million of biometric and identity records and giving the citizens with 8 million cards for voting purposes with fingertip crypt inside the card for identification at the electoral process.

Thank You Very Much for your attention!