



## The Demands of Real-World Biometric Identity Assurance Systems

Conor White, CTO, Daon

BCC 2004

### Headline News

THE WASHINGTON POST  
**Eight Airports to Test Biometric Defenses**

**Tech Security Arrives as the New Big Thing**  
 Steven I. Cooper, the Department of Homeland Security's chief information officer, had just wrapped up a speech at the government technology trade show ROSE last week when they began lining up: a dozen or so eager information security company executives making on-the-fly sales pitches.  
 To many of the executives, Cooper represents the billions of contracting dollars he represents are the ultimate pot of gold. Cooper joked that a hundred people told him they can solve all of the nation's cyber-security problems. Some of the department's staff members are looking at hundreds of proposals a week and

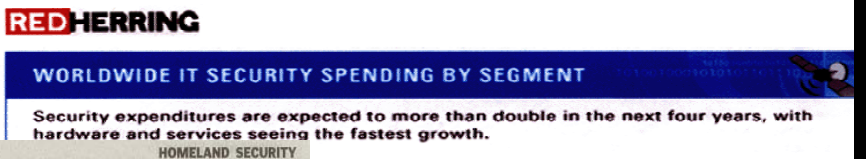
**FT FINANCIAL TIMES**  
**Caution Over Checkpoint Scheme**  
 Nearly three-quarters of US business travellers would not use a biometric checkpoint scheme, a survey shows.

Britain  
 The Economist May 1st 2004  
**Bagehot | A question of identity**

**THE TIMES**  
**All eyes on airport security.**  
 A Dutch... is using biometric testing for fast-track... How suit? Ros  
**TECHNOLOGY**  
**Biometrics moves to center stage**  
 09/23/02  
 By PATIENCE WAIT  
 Industry grows, but agencies rely primarily on fingerprinting solutions in the war on terrorism. Information capture suspected al Qaeda terrorists, they are required to take the detainee's fingerprints. It has not been used for fingerprinting. Instead, representatives of the FBI's Criminal Justice Information System (CJIS) are carrying around laptop computers and portable fingerprint capture devices to FBI offices in the United States, where they are testing the Integrated Automated Fingerprint Identification System, the nation's largest fingerprint database. True identities and whether they have been associated with other known terrorists are being used to enhance...

# NEWS BRIEFING

**Federal officials wrestle with homeland security problems**  
 BY SARITA CHOUREY, DIANE FRANK AND DIBYA SARKAR  
 Two Bush Cabinet secretaries sat side by side last week at a House Judiciary Committee hearing that pressed... that agencies still have ineffective plans that lack guidance, review and testing. "If [the Sept. 11 attacks were] the wake-up call, then we haven't seen the change when it comes to homeland security," said Tom Davis (R-Va.), chairman of the Government Reform Committee. Davis was at a hearing on the matter last week. Officials at the Federal Bureau of Investigation, which is leading the effort, responded. Later this week, the FBI will conduct a full-scale exercise, which they plan to complete by the end of the month. At least 45 federal agencies are involved in the exercise.



## The new face of biometrics

### Skin analysis

A class of pattern-recognition algorithms called surface texture analysis analyzes skin patches, such as those between the eyes or the cheek areas, for unique characteristics

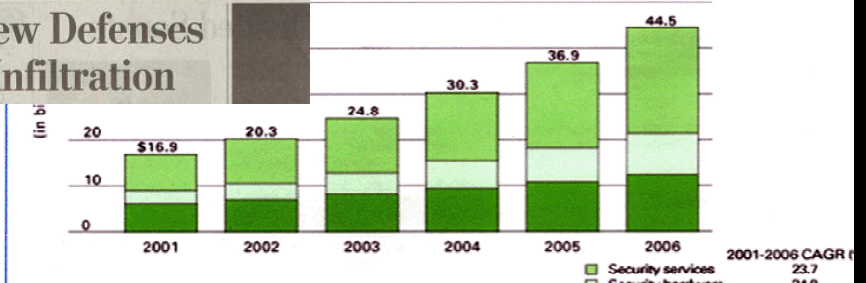
and can distinguish between identical twins. In facial recognition technology, feature analysis measures a person's features, such as the mouth, but it cannot distinguish between identical twins.



## Airports to Test New Defenses Against Terrorist Infiltration

- Measures mouth, eyes, and nose.
- Works with high- and low-resolution images.
- Surface texture analysis
  - Each person is unique.
  - Requires higher-resolution images.

Cybersecurity communications capability because of the ability to relocate and vital those sites.



# The Evolution of Biometric Identity Systems

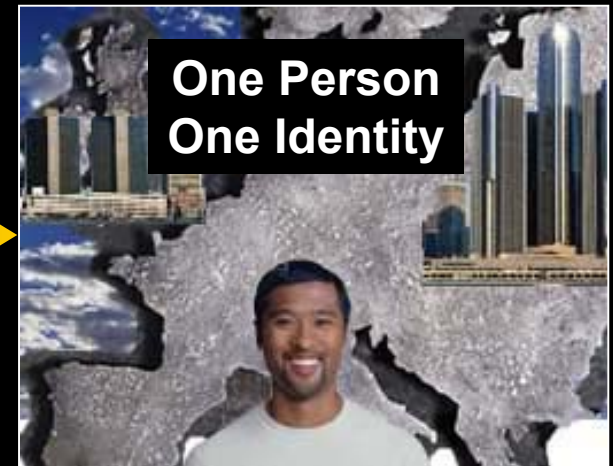
Government Systems Environment



**Biometric Identity Management**



The Vision



- Standard setting activity driven by government deployments
- Start with a flexible architecture
- Integrate with existing systems
- Create a service point for applications

# Real World is More Than a Biometric Match!

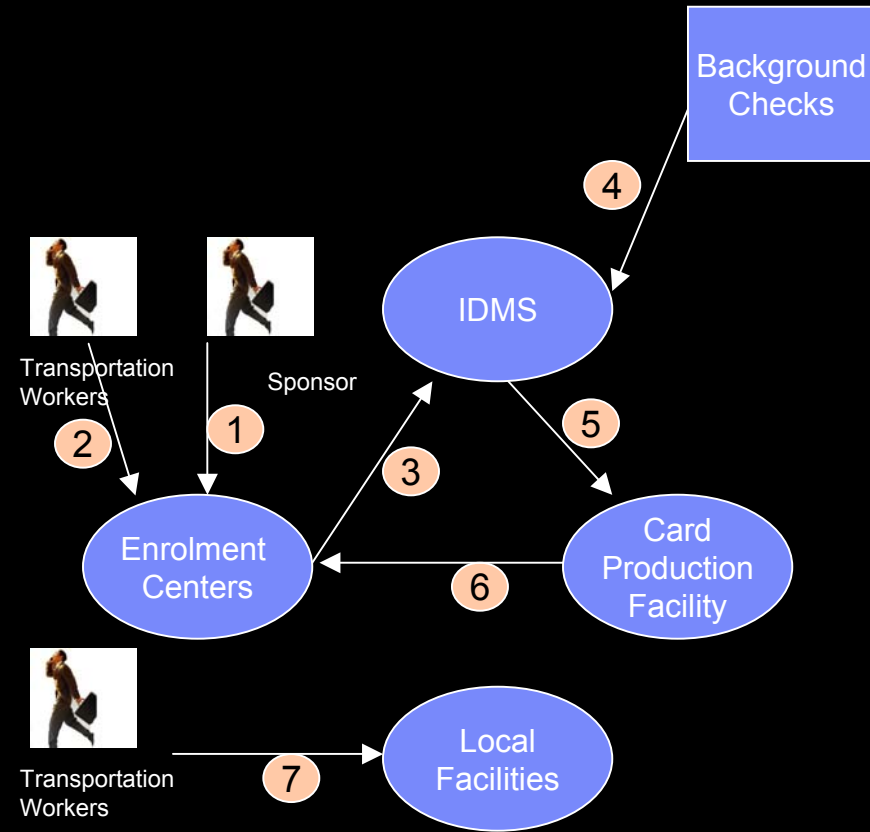
- Are biometrics accurate?  
Yes, but ... accuracy is dependent on many things – quality of enrolment, operational policies, choice of technologies and more.
- Do they enhance security?  
Yes, but ... they are only a component. Security is only as strong as the weakest link.
- Can they be used with large populations?  
Yes, but ... not everybody can provide a fingerprint, or an iris sample.
- Will they help secure my enterprise/country?  
Yes, but ... only if implemented as part of an overall Identity Assurance program in a Mission-Critical Infrastructure.

## Today's Challenge!

- Identity Assurance is more than a Biometric Match
  - Problem to be addressed has moved on from Biometric Performance (algorithms and devices)
- Business Process Efficiencies must be realized
- Some Key issues:
  - Operational System Performance (Variety of Stakeholders)
  - Integration with old and new business processes
  - Low risk, speed of deployment
  - Transition Management
  - Enhancing Security & Improving User Convenience
  - Addressing large, diverse populations
- Large Scale projects around the world are demonstrating that improved efficiencies together with enhanced security and convenience can be achieved

### TWIC in a Nutshell

- Pre-enrolment
- Enrolment
- Background check
- Notification & Scheduling
- Card Issuance
- Card Activation
- Verification
- Hot list Management
- Privacy and Security
- Physical Access
- Logical Access
- Finger, Face, Iris



## Registered Traveler Pilot in a Nutshell

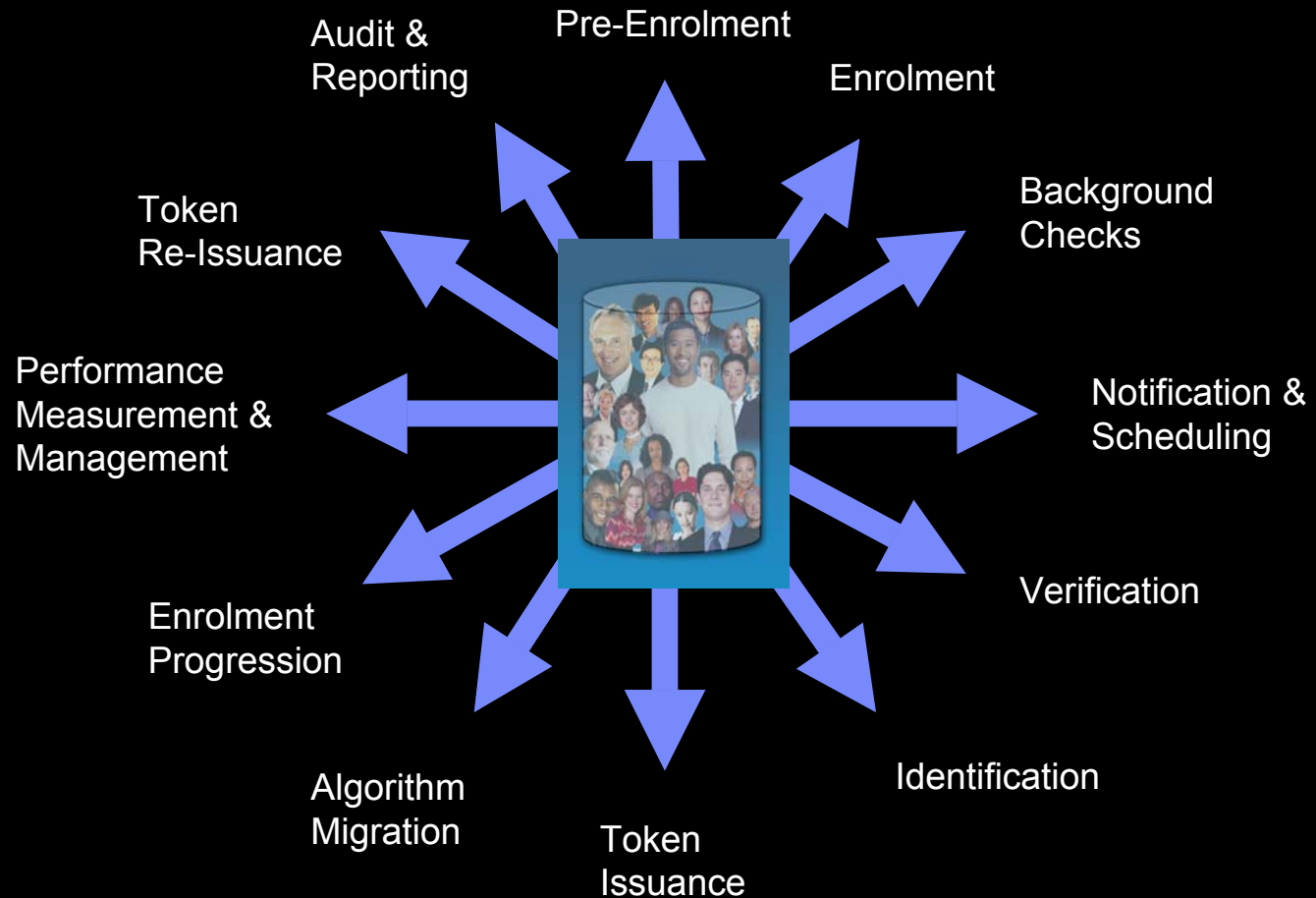
- Enrolment
- Background check
- Card Issuance (different cards)
- Verification
- Identification
- Kiosks
- Privacy and Security
- Finger, Iris



# Ten Challenges for Large Scale IA systems

1. Support the Identity Assurance Lifecycle
2. Provide Mission-Critical Quality of Service
3. Provide Flexibility of Business Process
4. Comply with Privacy Policy and Legislation
5. Standards Compliance
6. Deliver to Aggressive Timelines
7. Support Transition Management
8. On-going Management, Monitoring and Optimization
9. Support Program Evolution
10. Deliver Measurable Business Benefits

# 1. Supporting the Identity Assurance Life Cycle



## 2. Mission Critical Quality of Service



**Scalability - Volumes will be large**



**High Performance: Speed and Consistency**



**Availability: System reliability requirements**



**Security & Privacy will be paramount**

## 2a Characteristics of Scalable Systems

Cope with an ever increasing volume

Exponential Growth


Predictability

Flexible Deployment Model



**Scalability starts with architecture**  
**Demand proof of claims**

## 2b Characteristics of Availability



Constant availability is a claim that must be tested

System must leverage industry best practice

## 2c Characteristics of High Performance Systems

Rapid and consistent response time

Manages peak loads

Exploits high performing technologies

Measurement capabilities

## 2d System Security Characteristics



Focus on scheme security

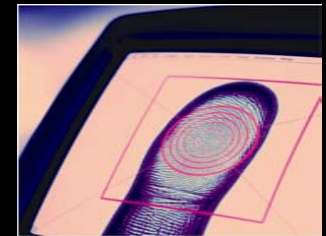
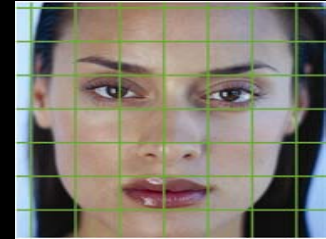
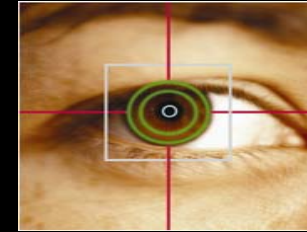
Use industry standard and best of breed encryption, key management, tamper resistant technologies

Make extensive use of digital signatures to implement non-repudiation

Ensure live-ness in each transaction

### 3. Flexibility of Business Process

- Identification vs Verification
- Centralized vs Distributed vs Federated
- Tokens – Magnetic Stripe, Smart Cards, RFID, National Id, Passports ...
- Biometric Fusion
- Build a Service Oriented Framework – Multiple Consumers
- Authentication Ubiquity – Match on Server, Match on Client, Match on Card.
- Integrated, Person-Centric Approach – Data Aggregation



### 4. Privacy Compliance

Fair and lawful use

Specified, accurate, up-to-date and explicit purpose

Respect for the right of the data subject

Data kept which permits identification for no longer than necessary

Proportionality: adequate, relevant and not excessive

Appropriate technical & organizational measures against unauthorized use or unlawful processing



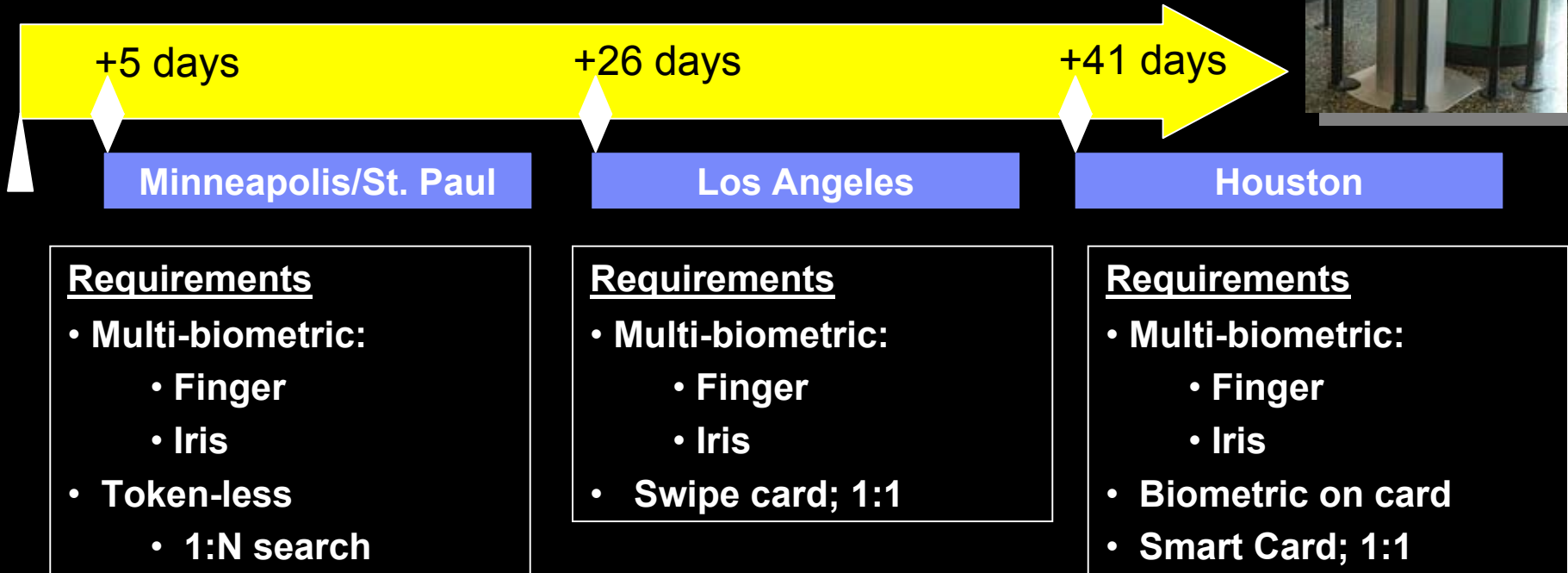
## 5. Standards Compliance

- Standards playing an increasingly important role
- Development of biometric standards and biometric application standards is proceeding at a pace!
- Standards will drive interoperability across all components of solution – for example:
  - Devices
  - Algorithms
  - Protocols
  - Application Integration
  - Data Capture and Storage



### 6. Increasingly Aggressive Timelines

Consider the Registered Traveler Pilot program:



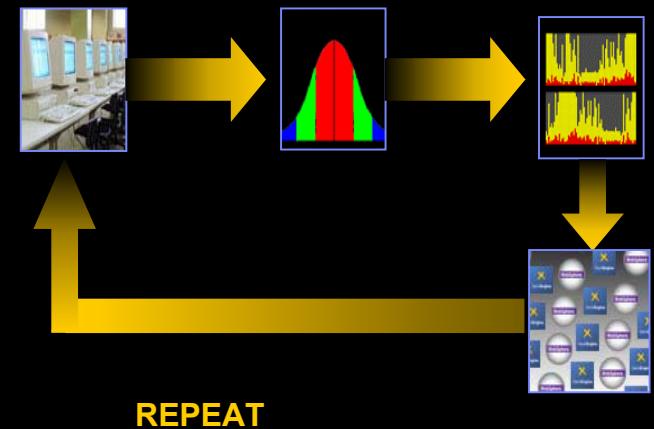
## 7. Key Challenges in Transitioning Operational Systems

- Implementation of Business Process in Dynamic Environments
- Increment Management (Non-disruptive growth)
- Balancing Operational Demands vs. Legacy Constraints
- Isolating Change to facilitate Technology Migration
- Providing flexibility to manage change
- Addressing emerging Operations & Maintenance challenges

*Supporting the life-cycle of solutions development*

### 8. On-going Management, Monitoring and Optimization

- Once deployed, a system must be monitored and managed
- Operational Tuning to suit population size and type
- Constant validation and ongoing testing of performance
- Extensive measurement and instrumentation
- Measure Business Process Improvements



## 9. Support Program Evolution

1,000's of users

10,000's of users

1,000,000's of users

**PHASE 1****Pilot**

Biometric Performance  
User Experience  
Technology Platform  
Quality of Service Assurance  
Component Level Security

**PHASE 2****Scaling Up**

Biometric Performance  
User Experience  
Technology Platform  
Quality of Service Assurance  
Component Level Security  
Privacy Protection  
Audit trail and Accountability  
Business Process  
Improvement  
Flexibility  
End to end scheme security

**PHASE 3****National & Intl**

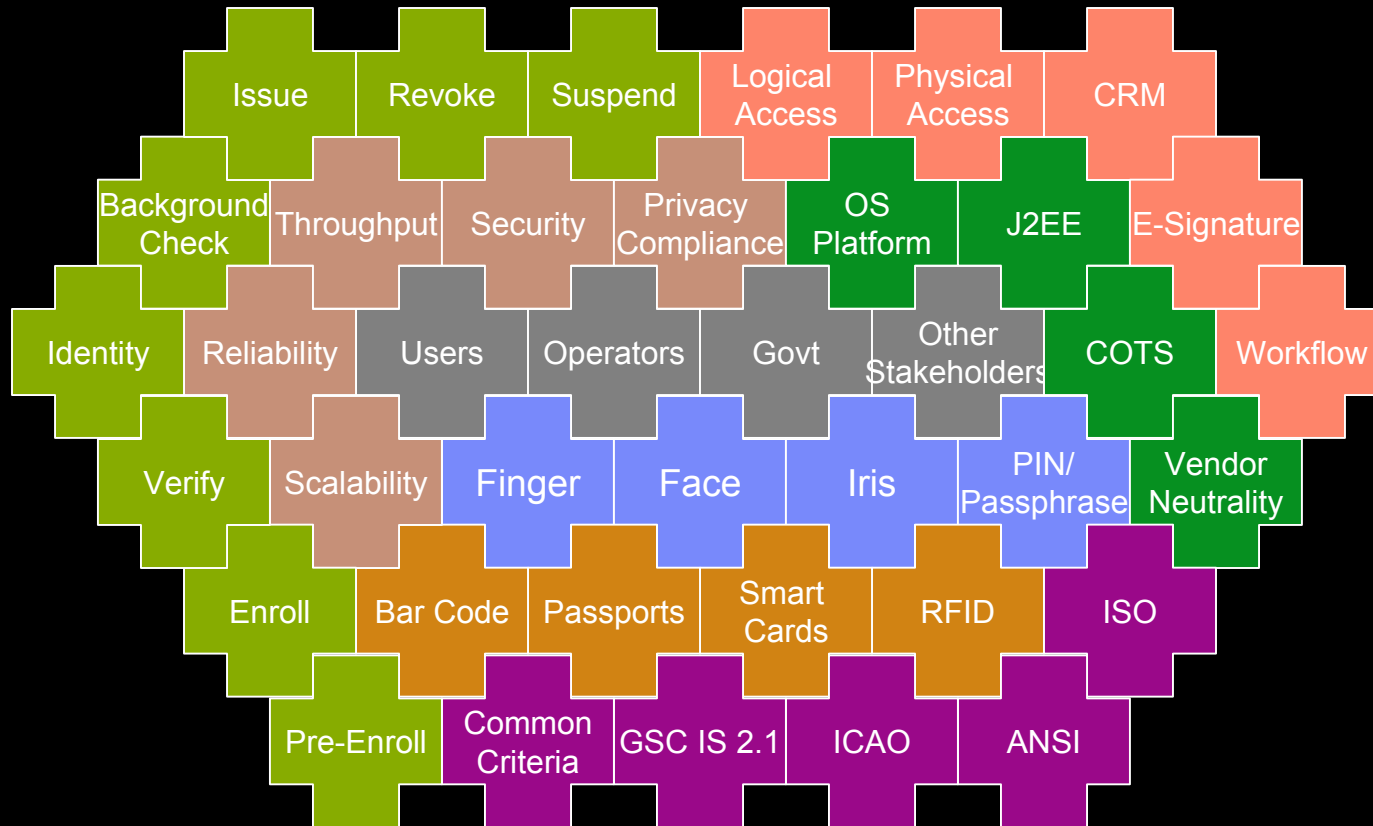
Biometric Performance  
User Experience  
Technology Platform  
Quality of Service Assurance  
Component Level Security  
Privacy Protection  
Audit trail and Accountability  
Business Process  
Improvement  
Flexibility  
End to End Scheme Security  
Predictive Growth Models  
Population Coverage  
Interoperability  
Standards Compliance

## 10. Measurable Business Benefits

- Original early implementations focused on security
- Security has an ROI (difficult to measure)
- Business Benefits
  - Queue Times
  - Process Efficiency
  - Automation
  - Staff Utilization
  - Stakeholder Perception
  - Customer Satisfaction
  - Privacy

As an industry we need start talking in terms of  
***Biometric Identity Assurance as an Enabler of Business Transformation.***

# The Requirements Jigsaw



**Thank You**

**[conor.white@daon.com](mailto:conor.white@daon.com)**