

Identity Management: Going Beyond Biometrics!

Presented by:
JOSEPH J. ATICK, Ph.D.
PRESIDENT AND CEO

Agenda

- I. Identity Management vs. Biometrics
- II. Identity Frameworks
- III. Program/System Integration
- IV. Role of Government

Situation Analysis

- Biometrics: Where are we?
 - Clear value proposition
 - Mandates
 - Myriad of Federal & International programs on horizon
 - Viable cost effective technologies
 - Standards developing rapidly
- But biometrics' promise is not yet fulfilled
 - Risks ahead in large scale implementations
 - Most critical time in history of Industry
 - Industry continues to lack a track record



Technology vs. Process

- So far: Biometrics Industry (not SIs or IT companies) has shouldered the burden of promoting adoption:
 - Disproportionate focus on technology issues
- A change in focus & attitude is needed
- Today's challenges:
 - Not technology
 - Process & system integration
 - Lowering deployment risk
- Role of biometrics at this point?

The Role of Biometrics

- Biometrics are critical for identity & security programs
- But must keep in mind Biometrics:
 - Are merely enabling technologies
 - Subservient to overall system requirements
 - NOT a security panacea
- Appropriate role: *enabling technologies that impose significant constraints on overall system design*



Looking at security from biometric end is tantamount to the “tail wagging the dog.”

Biometrics' Constraints?

- Still imperfect technologies
- Unfamiliar to end users
- Workflow changes
- Unproven scalability
- Data security issues
- Integration challenges
- Complex architecture
 - Remote distributed systems
 - Impact both client & server sides
- Raise legal & social issues (e.g. privacy)

Biometric complexity creates new opportunities for System Integrators & Component Providers

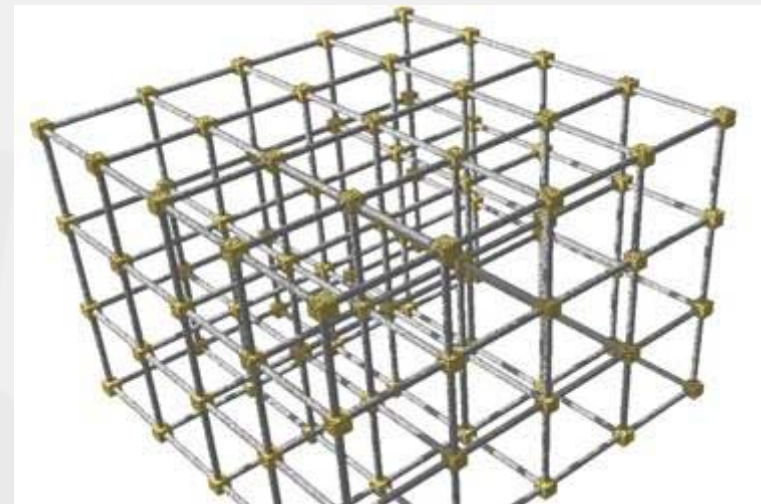
From Technology to Managing Identity

- Abstracting to a more fundamental level:
 - Human Identity
- *Managing Identity*
 - Myriad of issues & questions beyond FAR & FRR

Identity Capture	Uniqueness	Universality	Interoperability
Secure Storage	Secure Communication	Scalability	Flexibility
Business & Work Flow Interface	Privacy Assurance	User Acceptance	Overall TCO
Distributed Deployment	System Integrity	Performance	Advocacy

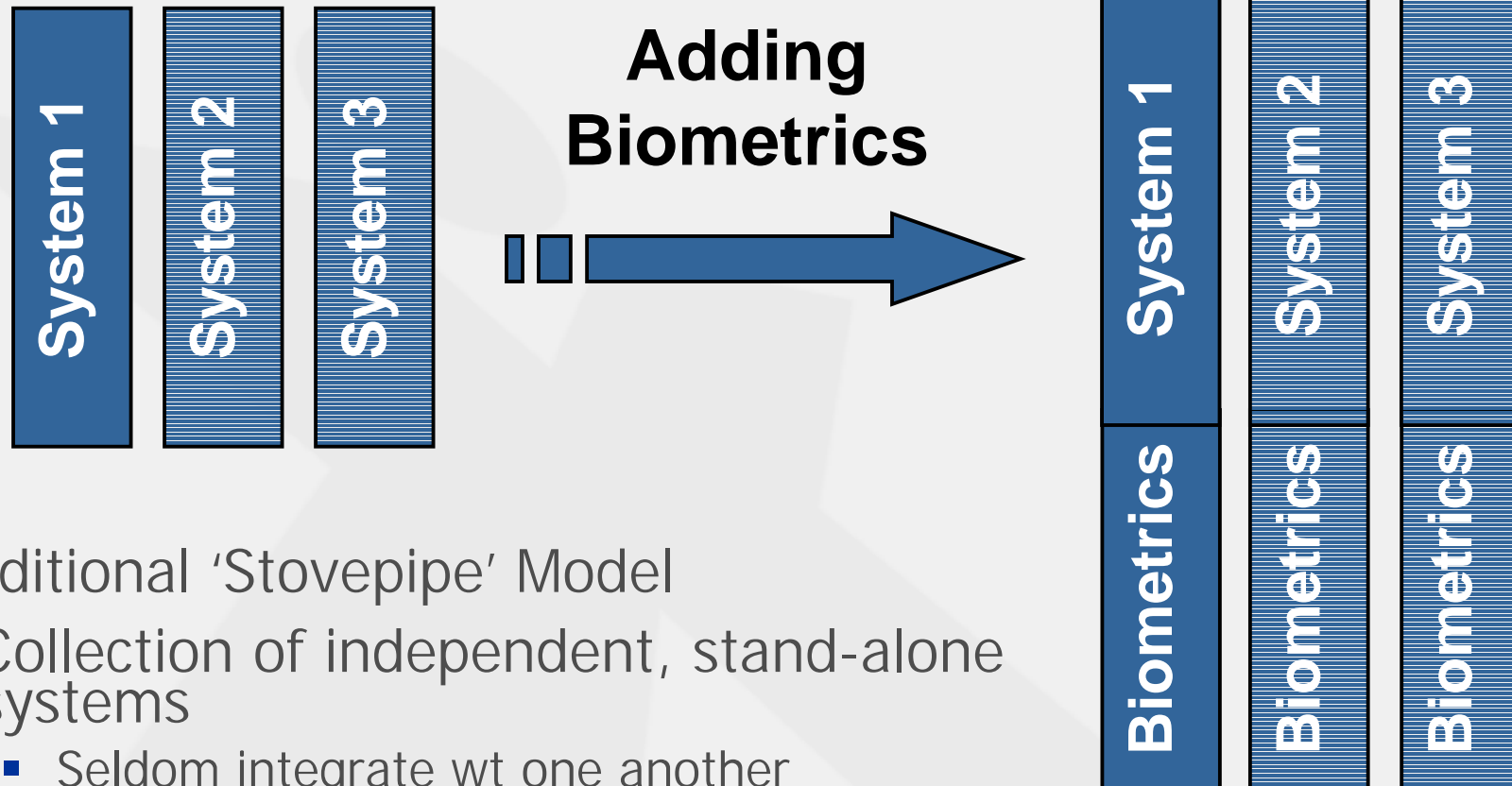
What is Needed?

- A framework for *Identity Management* where:
 - Above issues can be addressed
 - Best practices established
 - Higher level standards developed
- So what is an Identity Framework?



A New Framework
for Identity Is Needed

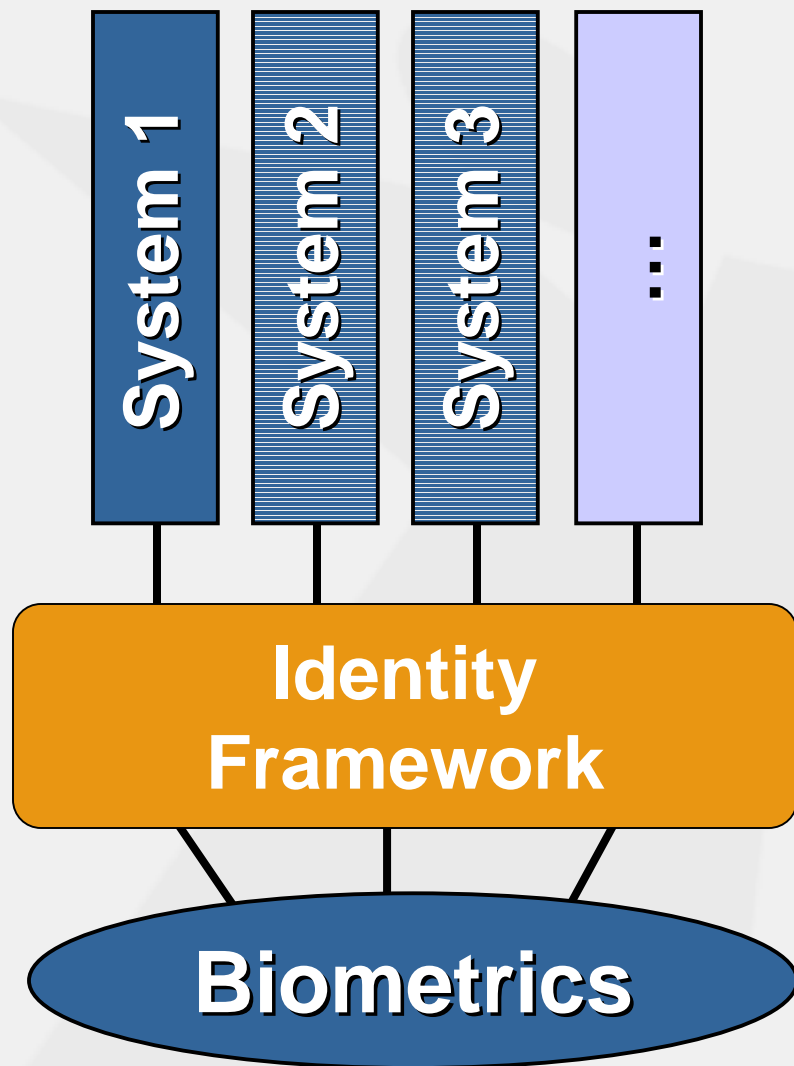
Traditional Approach to Identity



Traditional 'Stovepipe' Model

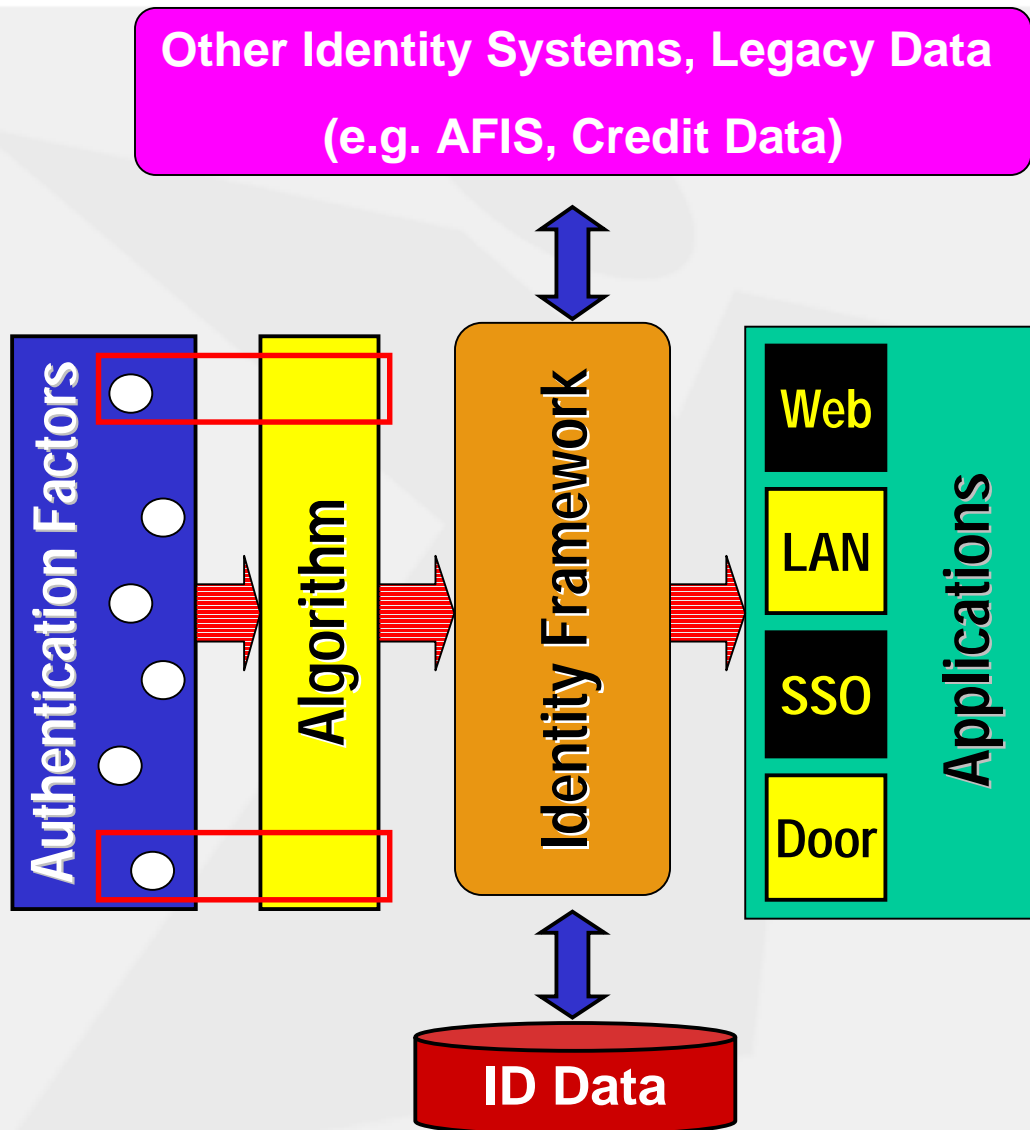
- Collection of independent, stand-alone systems
 - Seldom integrate wt one another
 - Significant redundancies
 - Many loop holes
 - Higher total cost of ownership

Employing Identity Framework



- Shared identity-related application services with well defined API
- Ties different components to create holistic systems
- Same Identity data served across different security applications
 - *Continuity of Identity*
 - *Universal Authentication*

Identity Framework: Connectivity

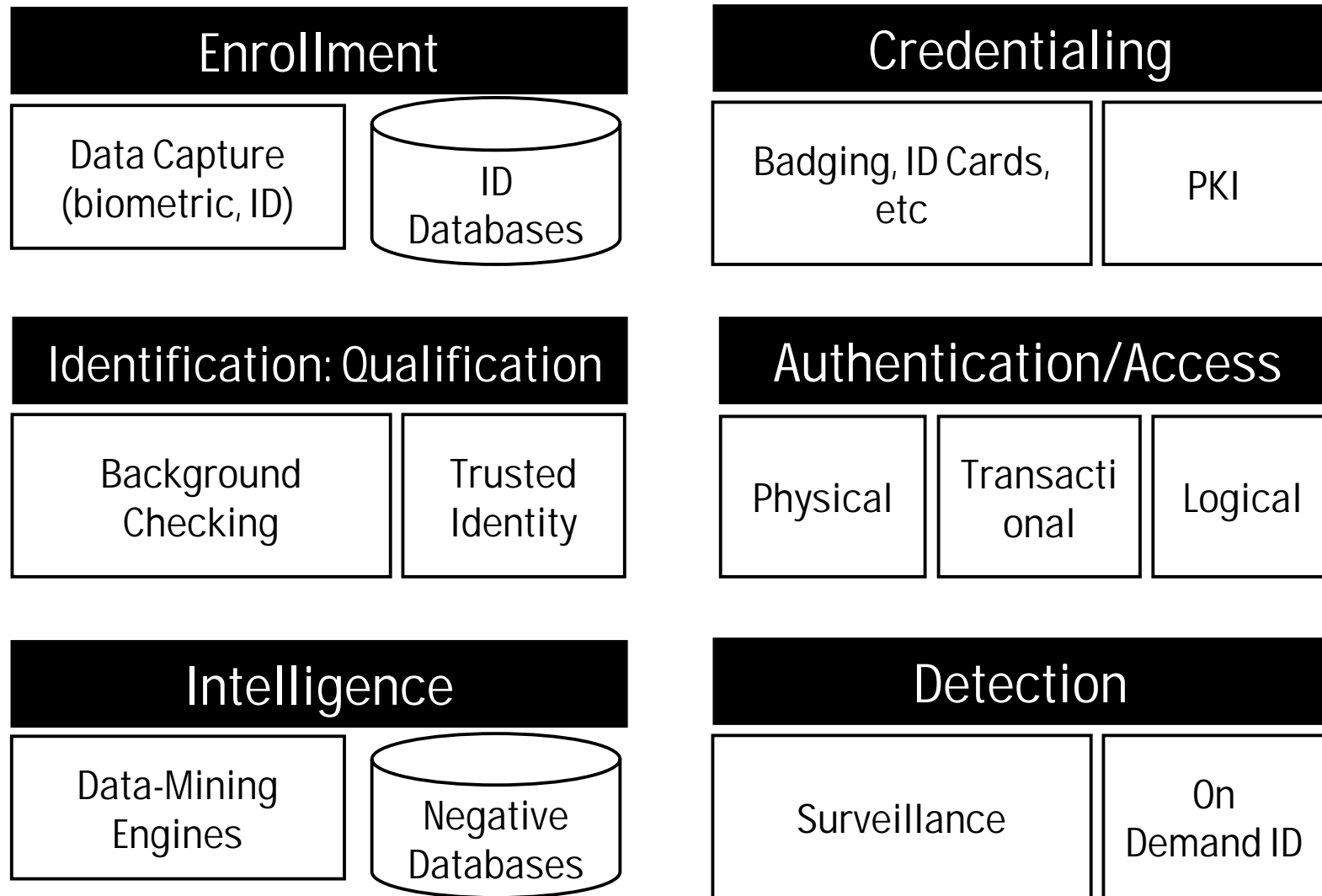


- Open to different factors, & applications
 - Evolution not revolution
 - Integrates wt Smart cards, passwords, tokens, etc
- Open standards for system interfaces
- Web-based components

Building an Identity Framework

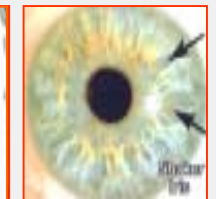
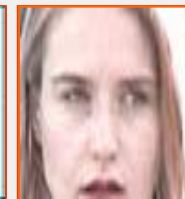
- Breaking down systems (enterprise, civil ID, user authentication) into stereotyped *Identity Processes*
 - Encapsulations of identity technology into higher level modules that can be addressed by application level system calls
 - Repeatable protocols common to most Identity systems
 - Actually subsystems (or even programs)
- Core Identity Processes?

Core Identity Processes



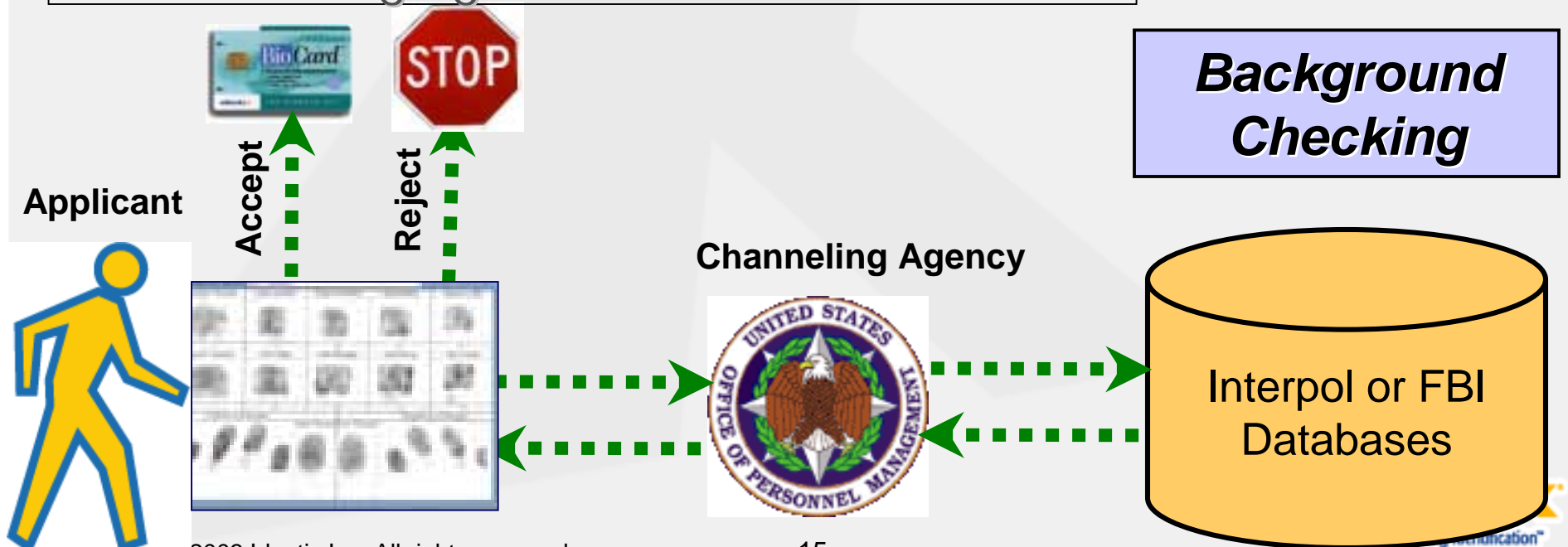
1. Enrollment

- Critical in any Identity program
 - Biometric & demographic data
 - Costly if not done right
- Challenges:
 - Typically distributed
 - Population touch point: 1st impression about biometrics
 - Data Quality
 - Data Integrity
 - Privacy: centralized vs. distributed
 - Open standards:
 - NIST images instead of proprietary templates
- Best practices?



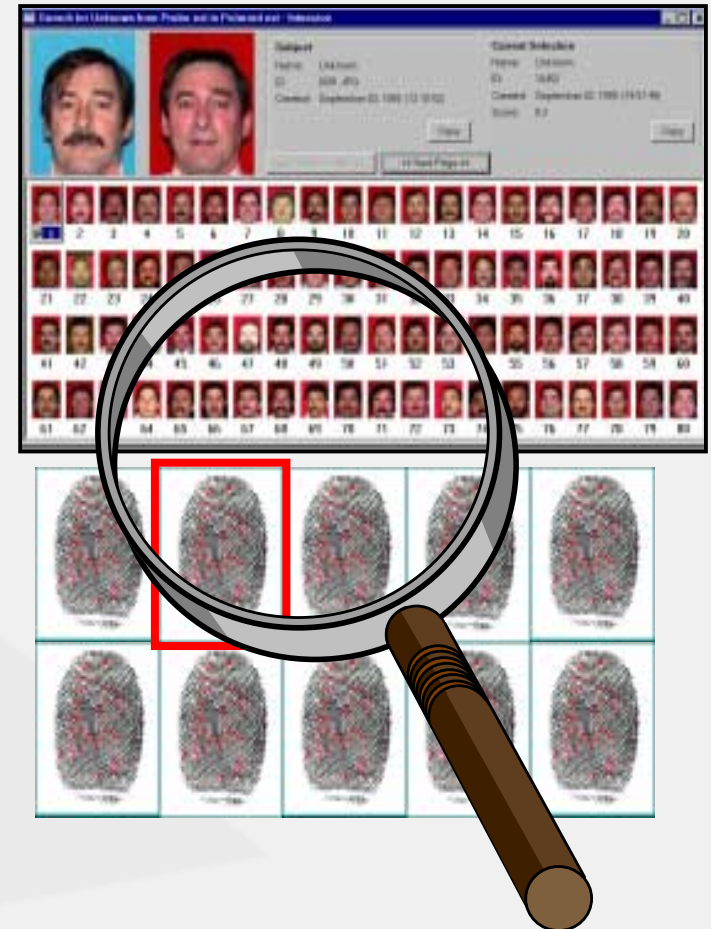
2. Identification: Qualification

- Two Questions:
 - Is Identity unique?
 - Can it be granted privileged status?
- Requires
 - 1-to-N against registration database
 - Matching against watchlists

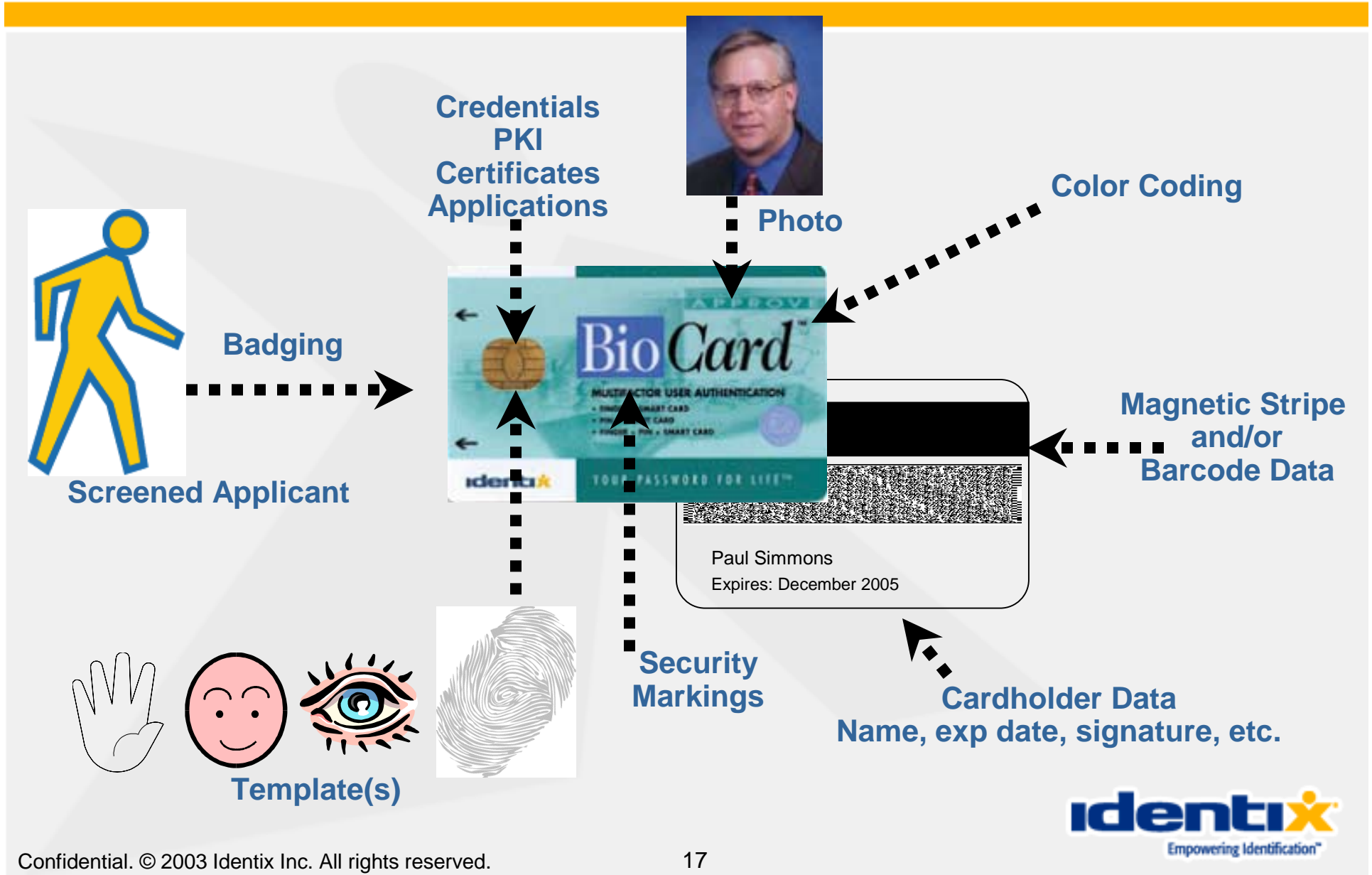


3. Intelligence

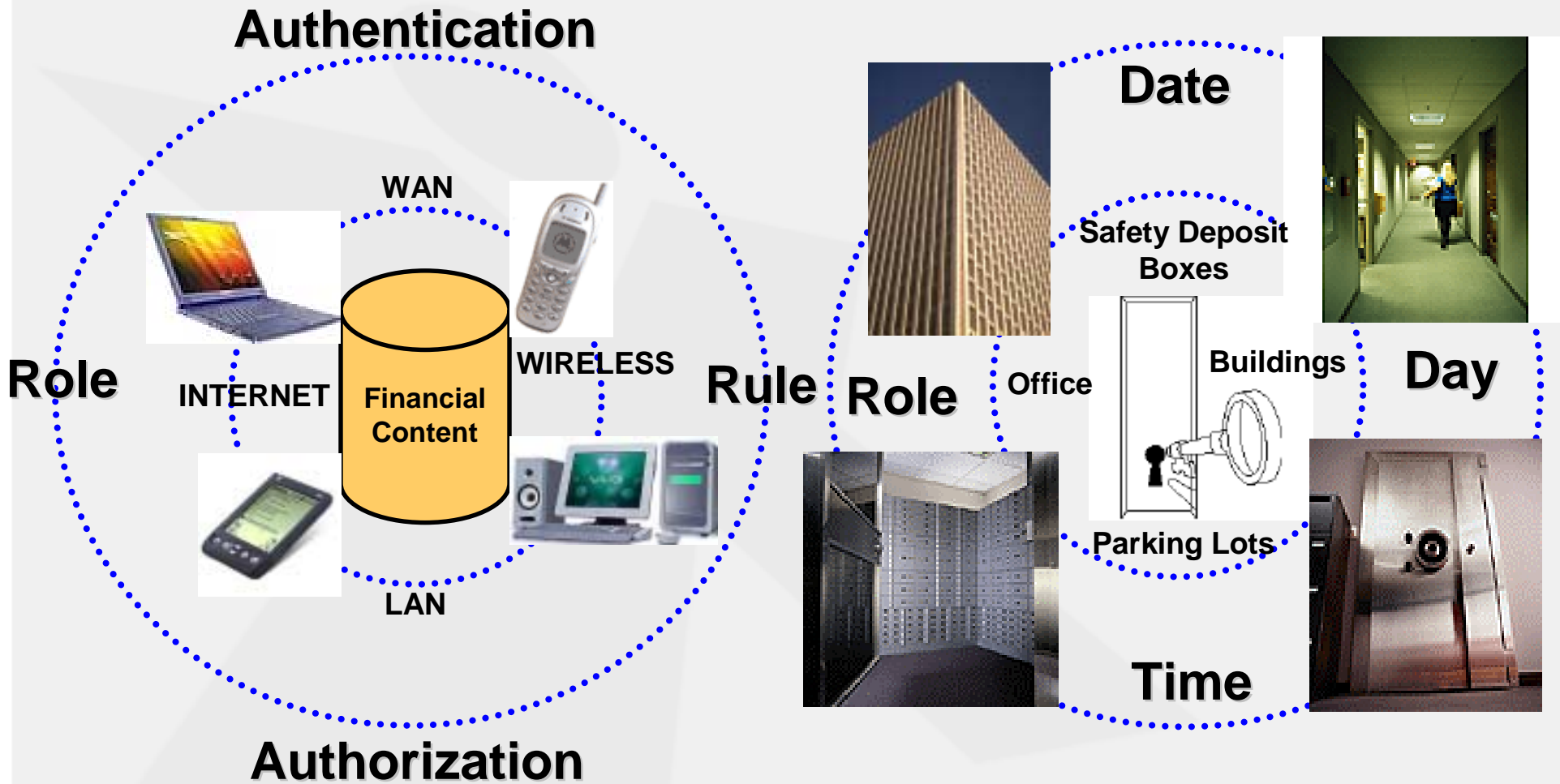
- Building & linking databases to uncover identities that could pose a threat
 - Watchlists
 - Terrorist Screening Center
 - 100,000 on watchlist already
 - TSA's "no-fly" list
 - US DOS "TIPOFF"
 - NCIC, etc
- Requires:
 - Data-Sharing:
 - Federal, State & Local, International
 - Data-Mining:
 - Multi-biometric technology platform
 - Link analysis
 - Standards:
 - Data formats & communication protocols or interfaces



4. Credentialing



5. Authentication

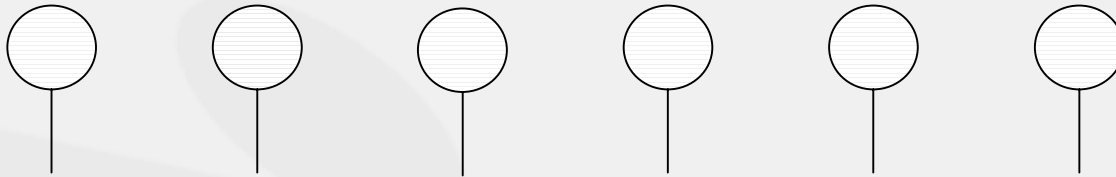


6. Detection

- Real-time detection against watch-lists
 - On demand screening:
 - Mobile Identification
 - Check point surveillance
 - Travel document screening
- Local law enforcement today has the leading expertise in detection:
 - Ontario, CA
 - Minneapolis, MN
 - Portland, OR



Identity Framework: Services



Enrollment Tools

Core
Identity
Technologies

Authentication
Tools

Identification
Engine Adapters

Identity
Policy
Management &
Enforcement

Identity
Storage
Adapters

Authentication
Device
Registry

Identity
Event
Auditing

Building Holistic Systems

- Adopt an Identity Framework as foundation
- Choose best of breed identity technologies & processes
- Choose a system integrator to pull overall system together
- Advantages:
 - More competitive solution
 - Better solution:
 - Flexible,
 - Scalable,
 - Interoperable,
 - Interchangeable
 - Incremental procurement
 - Spiral development
 - Leveraged investment



***Not locked
into vendor
proprietary
offering***

Alignment of Domain Expertise

- Ultimately identity modules could be elevated into identity programs
- ID Process specific domain expertise within industry & government
- Identity Services: alignment of identity processes with bureaus
- Examples:
 - Enrollment & Qualifications (front end): BCIS.
 - Qualification (back end): FBI
 - Credentialing: DOS, GSA, BMO, DMDC
 - Detection: DHS, Customs.
- The role of system integration: from integrating systems to integrating programs

Paradigm Shift: The Role of the SI

Yesterday

Technology
Companies

System requirements are becoming too complex:

- Integratability with legacy & interoperability
- Work flow considerations, E-Gov initiatives & Business Integration

TOMORROW

System
Integrators
with
expertise in
Business or
Program
Integration

The Opportunity for ID Management

ID Systems	Intelligence	BORDER CONTROL	VISAS	PASSPORTS
<p>(2) Civil IDs DMVs AAMVA M1 Standard</p>	<p>(0) Watchlists Criminal Databases Terrorist Databases Asylum Seekers Visa Fraud Applicants Custom Databases</p>	<p>(5) Entry/Exit Systems Throughout the World</p>	<p>(1) US VISIT Visas for non-VW nationals for Entry into US</p> <p>(4) Retaliation: Visas for US nationals visiting non VW countries</p>	<p>(3) US DOS: Smart Passports</p> <p>(2) Visa Waiver (VW) Nations: Smart Passports</p> <p>(0) ICAO Standards 9303: Face</p>

Think Global

- Remember: Identity management & Biometrics are about people
- USA
 - Validates biometrics.
 - Dominant market short term
- ROW
 - Dominant market in long run



FACT:
95% of
Earth's
population
lives outside
USA

What Industry Needs from Government

- Continued role in development & adoption of standards
- Validation and testing
 - Tests like FRVT & NIST
 - Building databases for testing (multi-modal data collection)
 - May require changes in law
- Certification activities
- Continued R&D
 - Biometric technologies are viable, but they are not yet mature
 - Without NSA, DARPA, DOJ, NIST, etc the biometric industry today would be a decade or two behind
- Unwavering commitment to programs despite Election Year Politics
- Addressing Privacy concerns

Privacy

- Privacy Pendulum over last 2 years
- Post 9/11 80% of People Polled
 - For Biometrics & ID Cards
- Majority of Privacy Issues with 'Patriot Act'
 - Wire Tapping, subpoenas, disclosure
- Biometrics Privacy Issues
 - System / Policy Level
 - Who owns the data
 - Who has access to the data
 - How to ensure data is not misused
 - Central Databases considered greatest threat to privacy



In Closing

- Have come a long way but more challenges are still ahead
- Process NOT technology
- Think identity not biometrics
- Embrace a framework for identity management as foundation in any large scale program
- Bite-size programs instead of mega-programs
- Interoperability among programs to build holistic systems

- Identity Management with biometrics will keep the industry and government busy for next decade!

Contact Information

Joseph J. Atick
President & CEO
Identix, Inc.

www.Indentix.com

(952) 932 0888 Corporate Office
(201) 332 9213 Research Center

Joseph.atick@Identix.com

**THANK
YOU FOR
YOUR
ATTENTION**