ISSEA

Identity - Privacy - Security

Systems Security Engineering and Privacy

Privacy and Security Workshop 3 Nov 2006

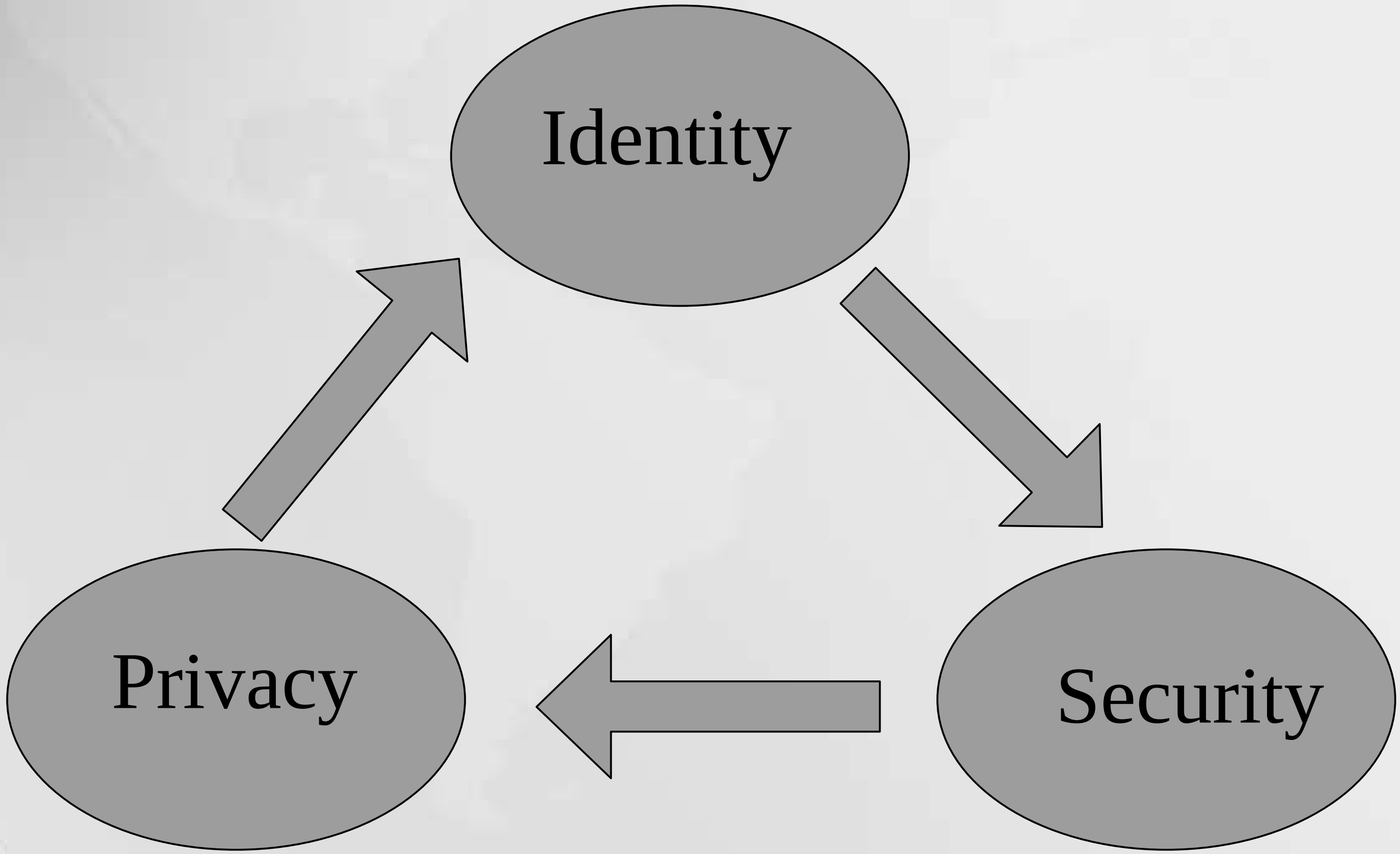
Toronto

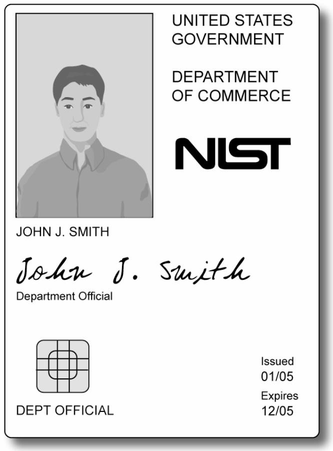
Overview

- Recent Motivation for Security Privacy Convergence
  - Digital Identity
  - FIPS 201
  - Border Security
  - in Financial Sector
  - Smart Cards – an enabling technology
- ISSEA / ISTPA Project
  - Guidance for Systems Security Engineering related to the ISTPA Framework
- Key References
  - ISTPA Framework
  - SSE-CMM – ISO IEC/DIS 21827
  - Network Applications Consortium Enterprise Security Architecture – Policy Driven Security Architecture
  - Common Criteria – ISO 15408
  - ISO/IEC TR 19791 – Security Assessment of Operational Systems
  - Privacy Impact Assessments
- Purpose of Guidance Document

Identity Management

The "Tipping Point" for Security and Privacy in support of the North American Security and Prosperity Partnership Program?





UNITED STATES
GOVERNMENT

DEPARTMENT
OF COMMERCE

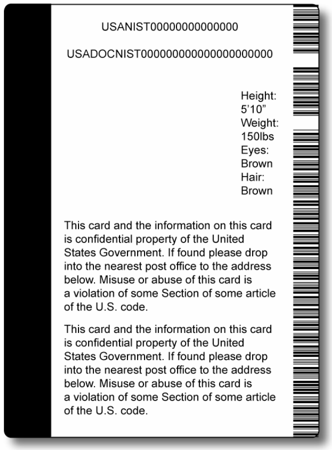
NIST

JOHN J. SMITH

John J. Smith
Department Official

Issued
01/05
Expires
12/05

DEPT OFFICIAL



USANIST00000000000000

USADOCNIST000000000000000000000

Height:
5'10"
Weight:
150lbs
Eyes:
Brown
Hair:
Brown

This card and the information on this card is confidential property of the United States Government. If found please drop into the nearest post office to the address below. Misuse or abuse of this card is a violation of some Section of some article of the U.S. code.

This card and the information on this card is confidential property of the United States Government. If found please drop into the nearest post office to the address below. Misuse or abuse of this card is a violation of some Section of some article of the U.S. code.

Personal Identity Verification Program

National Institute of Standards and Technology

Presidential Policy Driver

Homeland Security Presidential Directive 12

HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors (8/27/04)

http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

Federal Information Processing Standards (FIPS)

- Mandatory
- FISMA removed the waiver option
- In recent history, only two waivers had ever officially been requested and approved
- Technology advancements have contributed to the removal of waivers as more product developers are implementing the standards, increasing availability of compliant products especially in the area of encryption

HSPD #12
Key PIV Documents

- **HSPD-12**, Policy for a Common Identification Standard for Federal Employees and Contractors
- **OMB M-05-24**, Implementation of HSPD 12 - Policy for a Common Identification Standard for Federal Employees and Contractors
- **FIPS 201**, Personal Identity Verification for Federal Employees and Contractors
- **SP 800-73**, Interfaces for Personal Identity Verification
- **SP 800-76**, Biometric Data Specification for Personal Identity Verification
- **SP 800-78**, Cryptographic Algorithms and Key Sizes for Personal Identity Verification
- **SP 800-79**, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations
- **SP 800-85**, PIV Middleware and PIV Card Application Conformance Test Guidelines (Revision to permit transitional and end-point issuance system conformance certification)
- **NISTIR 7284**, Personal Identity Verification Card Management Report

Federal Information Processing Standard 201
Personal Identity Verification for Federal Employees and Contractors

- **Part I – Common Identification and Security Requirements**

  - HSPD 12 Control Objectives

    Examples: Identification shall be issued based on strong Government-wide criteria for verifying an individual employee's identity

    The identification shall be capable of being rapidly authenticated electronically Government-wide

  - Identity Proofing Requirements
  - Effective October 2005

- **Part II – Common Interoperability Requirements**

  - Specifications
  - Most provisions effective October 27, 2006
  - Implementation Timeframes IAW Agency Implementation Plans and OMB Memorandum M-05-24 of August 5, 2005

FIPS 201: Personal Identity Verification (PIV) Issued February 25, 2005

- Mandatory Prerequisites for Personal Identity Verification (PIV) Card Issuance
- Mandatory and Optional PIV Card Visual Data
- Mandatory and Optional PIV Card Electromagnetic Elements
- Mandatory and Optional PIV Electronically Stored Data
- Minimal Card Information Available for “Free Read”
- Large population – affects every Federal government employee and eligible contractors (~ 10M+)

FIPS 201 REQUIREMENTS

PIV Card Visual Data

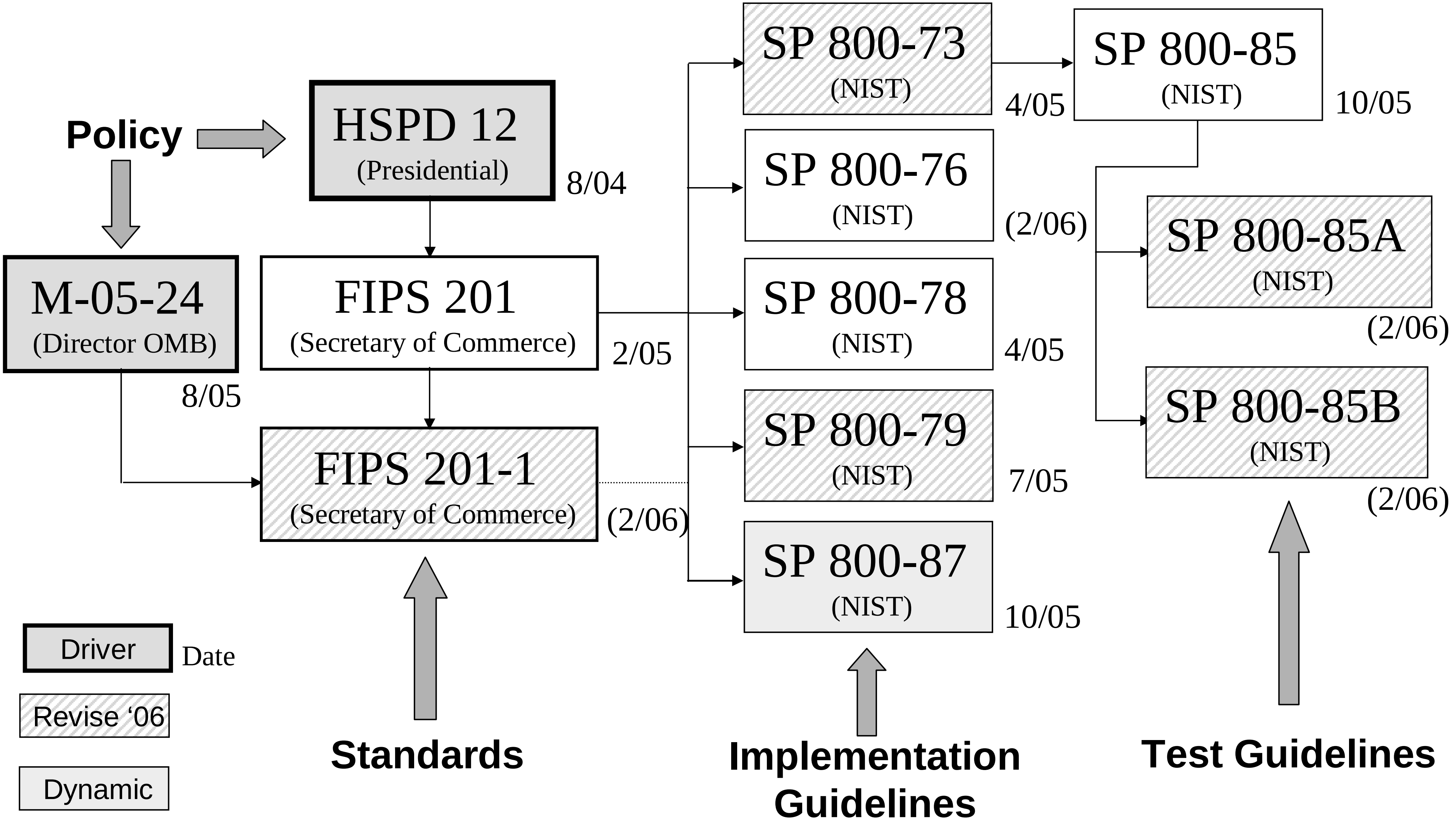
Mandatory

- Name
- Employee Affiliation
- Card Expiration Date
- Card Serial Number (Unique to Issuer)
- Issuer Identification

Optional

- Card Holder’s Written Signature
- Pay Grade
- Rank
- Agency Name and/or Department
- Agency Seal
- Issue Date
- Information for Returning Lost Card
- Color codes
- Federal Emergency Official Designation

HSPD #12
PIV Document Relationships



Policy

HSPD 12
(Presidential)
8/04

M-05-24
(Director OMB)
8/05

FIPS 201
(Secretary of Commerce)
2/05

FIPS 201-1
(Secretary of Commerce)
(2/06)

SP 800-73
(NIST)
4/05

SP 800-76
(NIST)
(2/06)

SP 800-78
(NIST)
4/05

SP 800-79
(NIST)
7/05

SP 800-87
(NIST)
10/05

SP 800-85
(NIST)
10/05

SP 800-85A
(NIST)
(2/06)

SP 800-85B
(NIST)
(2/06)

Driver Date

Revise ‘06

Dynamic

Standards

Implementation Guidelines

Test Guidelines

Border Security – Global Initiatives

- North America
  - **US Visit (USA)**
  - **USCIS Transformation (USA)**
  - **TSA Passenger security screening process (USA)**
  - **Integrated Automated Fingerprint Identification System (IAFIS) (USA)**
  - **Global Case Management System**
  - **Realtime Identification System (Can)**
  - **National Routing System (Can)**
  - **Facial Recognition System (Can)**
  - **Transportation Workers Identity Credential (TWIC)**
  - **TSA Registered Traveler – (USA)**
  - **International Registered Traveler USA/Netherlands**
  - **CANPASS (Can)**
  - **Nexus (Can/US)**
  - **Secure Electronic Network for Traveler Rapid Inspection (SENTRI) (Mexico-USA) US Passenger Accelerated Service (US Pass – (US PASS) (USA)**
  - **Western Hemisphere Travel Initiative (USA)**

Border Security – Global Initiatives

- Europe
  - Schengen Information System II (SIS II) EU
  - Visa Information System II (VIS II) EU
  - EURODAC (EU)
  - eBorders UK
  - IRIS Recognition System (IRIS) UK
  - Semaphore – UK
  - Rail Passenger Screening – UK
  - Garda National Immigration Bureau System (GNIB) Ireland
  - Simplified Passenger Travel Interest Group (SPTIG) EU
  - Pegase – France
  - Privium – Netherlands
  - Frankfurt Airport – Germany
  - UK National ID – UK
  - France National ID France
  - False and Authentic Documents (FADO – EU)

Border Security – Global Initiatives

- Asia Pacific
  - Advanced Passenger Processing (APP) Australia
  - DIMIA Immigration Biometrics Integration Australia
  - Electronics Travel Authority System (ETAS) Australia
  - Advanced Passenger Screening (APS) New Zealand
  - Automated Border Crossing – New Zealand
  - Automated Passenger Clearance APC HongKong
  - Japan Visit – Japan
  - Automated Biometrics Clearance Pilot – Japan
  - Japan e-Airport Japan
  - Fully Automated Seamless Travel (FAST) – Singapore
  - MyKad - Malaysia

Financial Sector Initiatives

- Payment Card Industry (PCI) PIN Entry Device (PED) - program to meet Visa, MasterCard and JCB requirements – Global markets
- PCI Data Security Standard (DSS) aimed at members, merchants and vendors who process, transmit or store cardholder data – Global markets
- MasterCard Point of Sale (POS) Terminal Security Program (PTS) - program aimed at devices with TCP/IP protocols and security services – Global markets
- ISO 15408 – Common Criteria (CC) – evaluations of devices to meet Protection Profiles defined by organization such as APACS (the UK payment association) and BITS Financial Services Roundtable (US financial sector) Test Mark program
- Interac Device Certification – for ATM and POS devices targeted at the Canadian Market

Smart Card Technology –

International Smart Card Industry Association

- 2.6 billion cards shipped in 2005 and shipments of nearly 3 billion are expected for 2006
- Smart Cards in Government and Health grew by 25%
- Financial Services, retail and loyalty grew 20%
- Telecom sector grew 19%

Smart Cards – an enabling technology for Digital Identity *

“Smart cards can provide authenticated and authorized information access, implementing a personal firewall for the individual and releasing only the information required when the card is presented. Smart card technology provides strong privacy-enabling features for ID system designers, including the ability to:

- Support anonymous and pseudonymous schemes
- Segregate multiple applications on the card
- Support multiple single-purpose IDs
- Provide authentication of other system components
- Provide on-card matching of cardholder verification information
- Implement strong security for both the ID card and personal data

Smart cards provide solutions that can enhance privacy protection and guard against identity theft in different ID system architectures.”

*Smart Card Alliance

Operation of Interac - CA

EWA-Canada Ltd. is pleased to announce that we have been selected by Interac Association to establish and operate an EMV-compliant Certificate Authority (CA) in Canada to support the *Interac* Shared Services in a new Chip environment. Additionally, we will assist Interac Association with the establishment of a Registration Authority (RA) to be operated by the Association for Issuers.

Operating together, the CA and RA will contribute to the proper management of the Public Key Certificates required for the *Interac* Shared Cash Dispensing at ABMs and *Interac* Direct Payment at Points-of-Sale in a Chip environment.

EWA-Canada was selected following a competitive process in part because of our extensive background in this field and our credentials as a Trusted Third Party service provider.

Operation of Interac - CA

EWA-Canada Ltd. is pleased to announce that we have been selected by Interac Association to establish and operate an EMV-compliant Certificate Authority (CA) in Canada to support the *Interac* Shared Services in a new Chip environment. Additionally, we will assist Interac Association with the establishment of a Registration Authority (RA) to be operated by the Association for Issuers.

Operating together, the CA and RA will contribute to the proper management of the Public Key Certificates required for the *Interac* Shared Cash Dispensing at ABMs and *Interac* Direct Payment at Points-of-Sale in a Chip environment.

EWA-Canada was selected following a competitive process in part because of our extensive background in this field and our credentials as a Trusted Third Party service provider.

Operation of Interac - CA

EWA-Canada Ltd. is pleased to announce that we have been selected by Interac Association to establish and operate an EMV-compliant Certificate Authority (CA) in Canada to support the *Interac* Shared Services in a new Chip environment. Additionally, we will assist Interac Association with the establishment of a Registration Authority (RA) to be operated by the Association for Issuers.

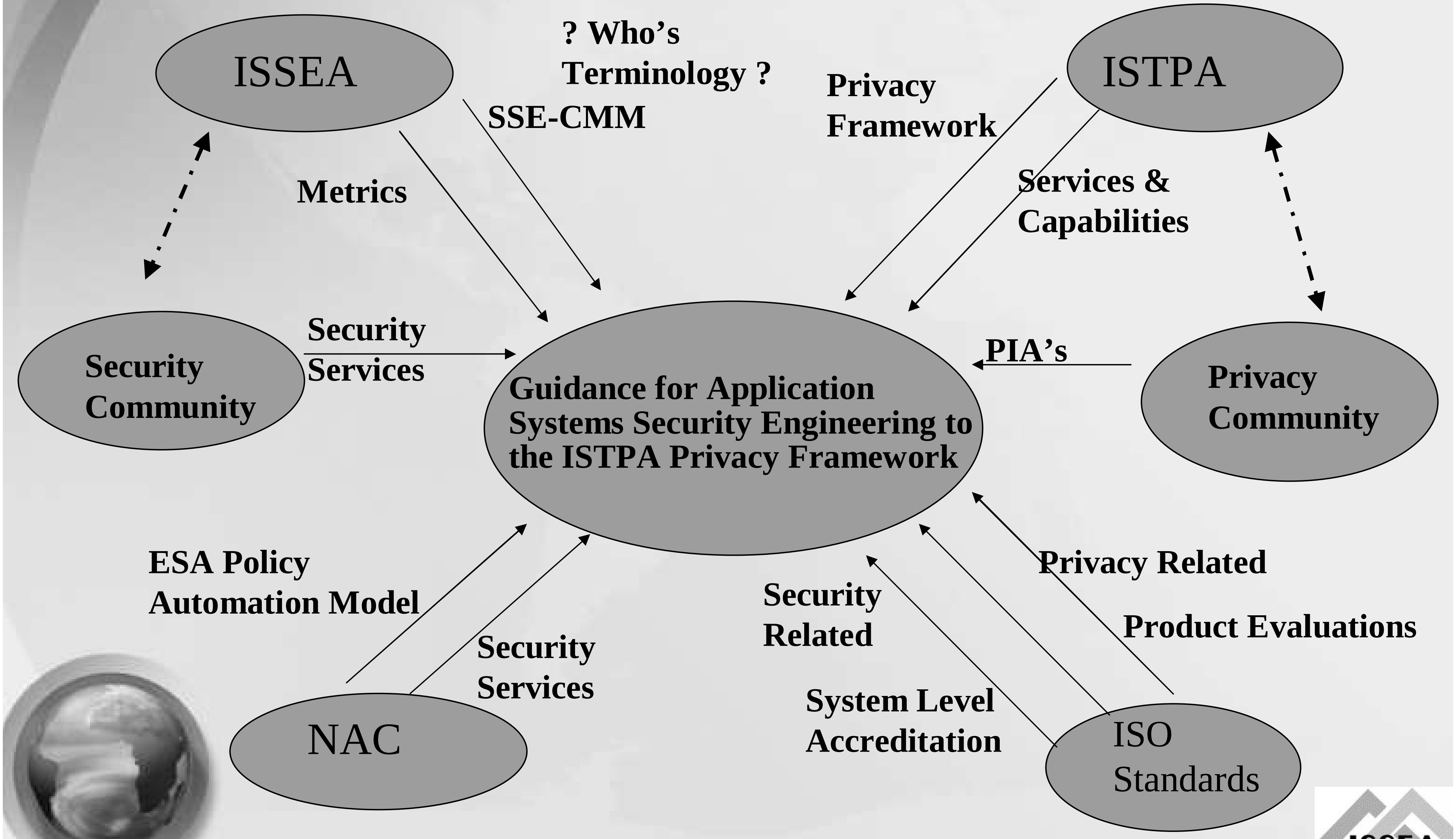
Operating together, the CA and RA will contribute to the proper management of the Public Key Certificates required for the *Interac* Shared Cash Dispensing at ABMs and *Interac* Direct Payment at Points-of-Sale in a Chip environment.

EWA-Canada was selected following a competitive process in part because of our extensive background in this field and our credentials as a Trusted Third Party service provider.

Guidance for Application of Systems Security Engineering to the ISTPA Privacy Framework

- Purpose:
  - The purpose of this document is to provide a security engineering perspective of the “privacy services and capabilities” defined by the ISTPA framework document and demonstrate:
    - how the systems security engineering base practices defined by the SSE-CMM can be used to develop, deliver and operate a system to comply with all relevant policies; and
    - how the resulting system architecture can be assessed to provide assurance that both security and privacy requirements have been met.

Privacy & Security Convergence



? Who's Terminology ?

ISSEA

ISTPA

SSE-CMM

Privacy Framework

Metrics

Services & Capabilities

Security Community

Security Services

Guidance for Application Systems Security Engineering to the ISTPA Privacy Framework

PIA's

Privacy Community

ESA Policy Automation Model

Security Services

Security Related

Privacy Related

Product Evaluations

System Level Accreditation

NAC

ISO Standards

Enterprise Security Architecture

– An Overview

Keith T. Hall
Sr. Member of the Professional Staff
SRA International
Keith_Hall@sra.com
(202) 255-8761

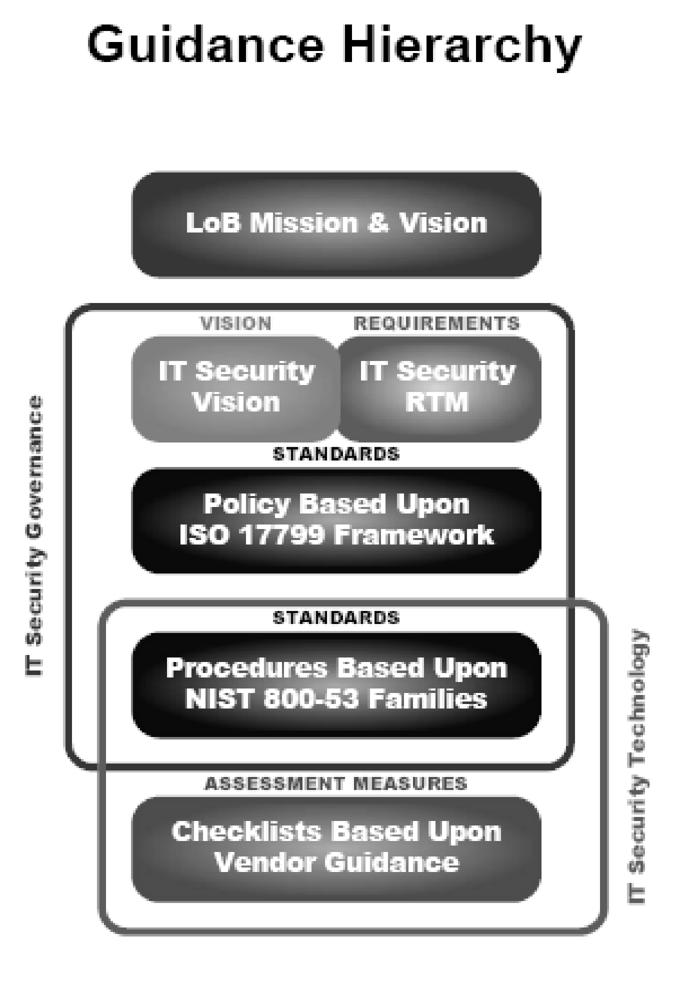
MBA, BSEE, INFOSEC Professional (NSTISSI 4011 Std), Senior Systems Manager (CNSSI 4012 Std), CISSP-ISSEP, CISA, IAM, IEM

Prior Cisco IP Telephony Support Specialist, Cisco IP Telephony Design Specialist, CCSP, CCIP, CCDP, CCNP, CCDA, CCNA, CSS-1, MCT, MCSE, MCP-SI

ISSEA

ESA - Background

- Objectives of *NAC's Enterprise Security Architecture: A Framework and Template for Policy-Driven Security:*
  - Provide a framework that serves as a common reference for describing enterprise security architecture and technology both within and between organizations.
  - Provide a template that allows user organizations to select the elements of enterprise security architecture they require and to tailor them to their needs.



Guidance Hierarchy

LoB Mission & Vision

IT Security Governance

VISION

IT Security Vision

REQUIREMENTS

IT Security RTM

STANDARDS

Policy Based Upon ISO 17799 Framework

STANDARDS

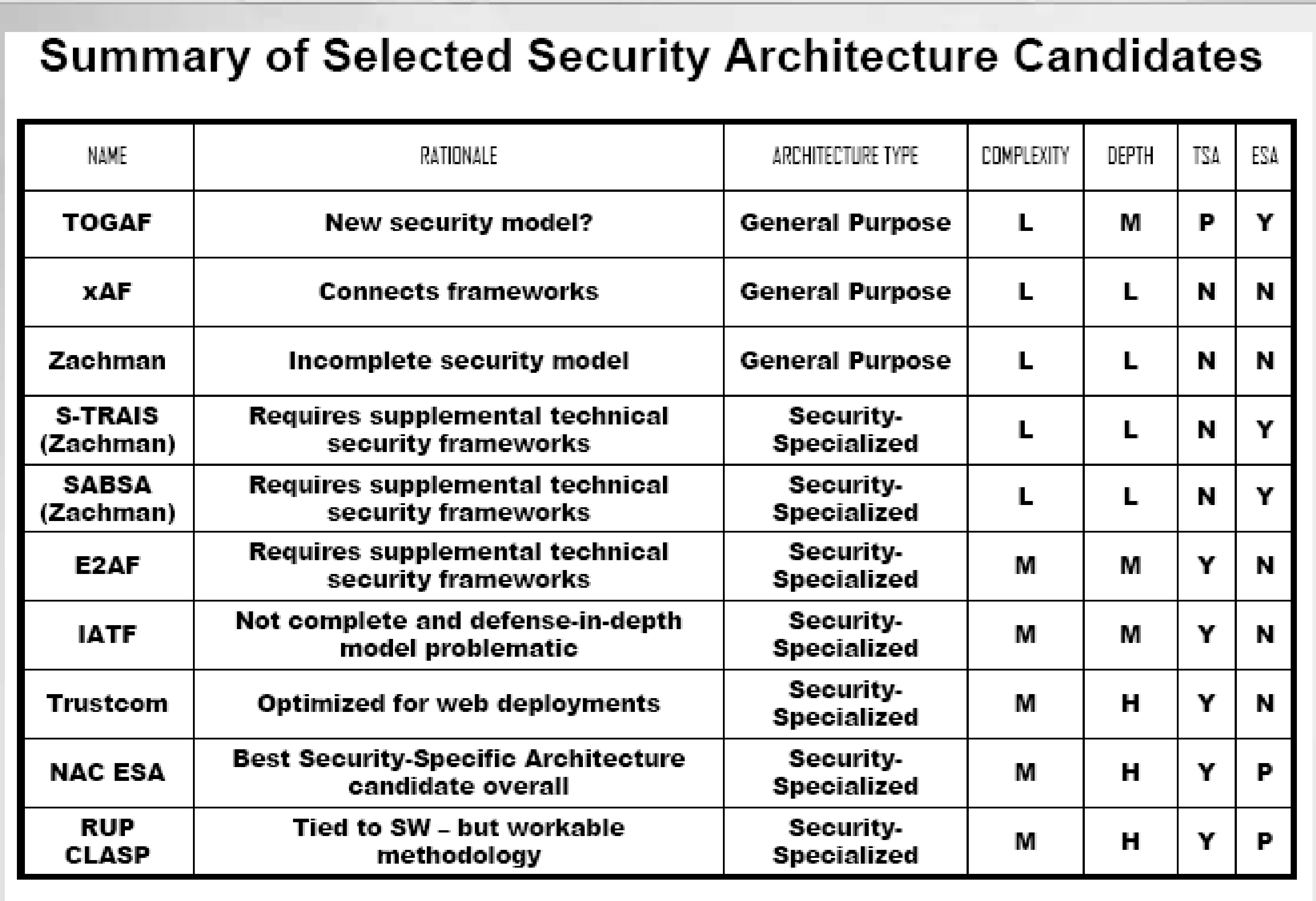
Procedures Based Upon NIST 800-53 Families

IT Security Technology

ASSESSMENT MEASURES

Checklists Based Upon Vendor Guidance

Best Security Specific Architecture



Summary of Selected Security Architecture Candidates

NAME	RATIONALE	ARCHITECTURE TYPE	COMPLEXITY	DEPTH	TSA	ESA
TOGAF	New security model?	General Purpose	L	M	P	Y
xAF	Connects frameworks	General Purpose	L	L	N	N
Zachman	Incomplete security model	General Purpose	L	L	N	N
S-TRAIS (Zachman)	Requires supplemental technical security frameworks	Security-Specialized	L	L	N	Y
SABSA (Zachman)	Requires supplemental technical security frameworks	Security-Specialized	L	L	N	Y
E2AF	Requires supplemental technical security frameworks	Security-Specialized	M	M	Y	N
IATF	Not complete and defense-in-depth model problematic	Security-Specialized	M	M	Y	N
Trustcom	Optimized for web deployments	Security-Specialized	M	H	Y	N
NAC ESA	Best Security-Specific Architecture candidate overall	Security-Specialized	M	H	Y	P
RUP CLASP	Tied to SW – but workable methodology	Security-Specialized	M	H	Y	P

ISSEA

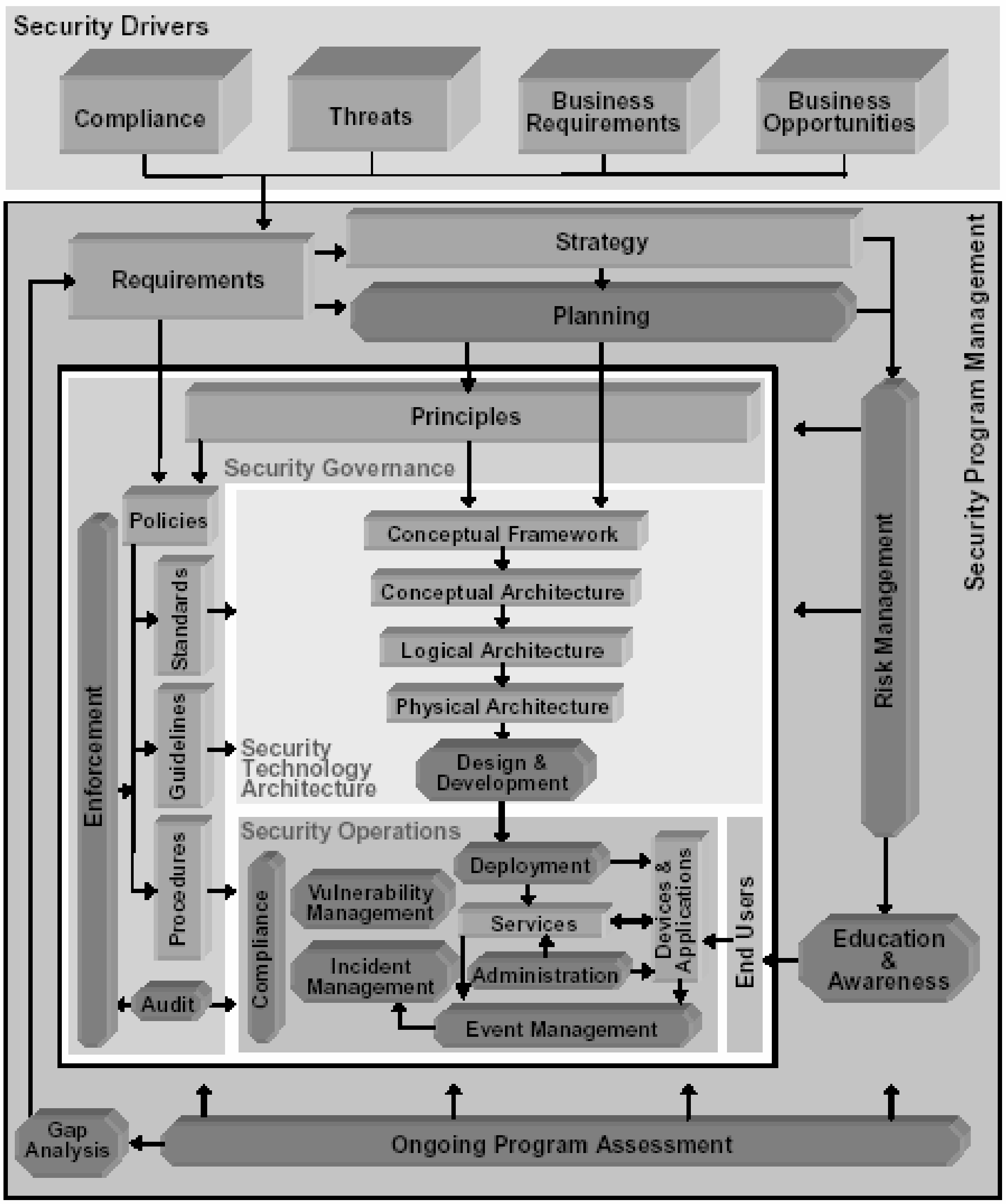


Figure 3. Enterprise Security Program Framework

Challenges

- The search for a common language
  - “security services” – no common definition
  - Emotional baggage related to “security” and “Privacy”
- Value of deliverable –
  - Needs to be of use to systems engineers who need to understand scope, context and issues related to legacy systems and new systems
- Need relevant examples (use-cases) that relate to international audience and their priorities
  - Digital Identities – the virtual border

Identity Management

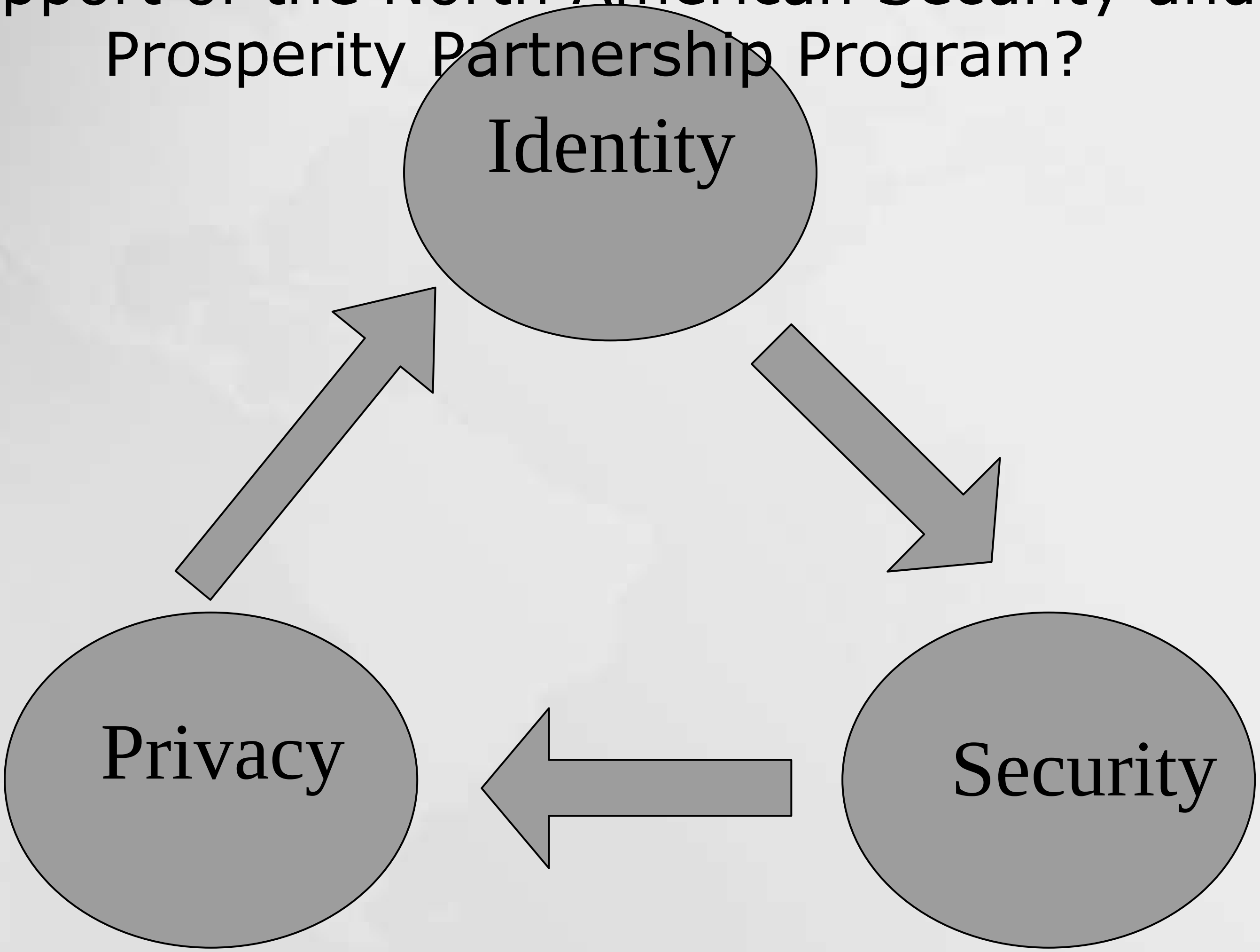
- “The time has come the Walrus said to talk of many things, of shoes and ships and sealing way and whether pigs have wings”

- US could shut Canada border over bird flu – the journal of Commerce – 4 May, 2006

- “Tipping Point – is that magic moment when an idea, trend or social behavior crosses the threshold, tips and spreads like wildfire”

Identity Management

The "Tipping Point" for Security and Privacy in support of the North American Security and Prosperity Partnership Program?



- Questions
- jrobbins@ewa-canada.com