ITU-T Workshop on Addressing Security Challenges on a Global Scale

6 - 7 December 2010 Geneva, Switzerland
A Service and Functions-Based Reference Model for Data Privacy

John Sabo, CA Technologies
Co-Chair, OASIS PMRM TC
John.t.sabo@ca.com
Critical Privacy Drivers and Issues

• Networks and the PI Lifecycle
  – Digitally-based personal information is networked and boundless

• Principles/Legislation/Policies
  – Security and Privacy Integration expected
  – Compliance - and increased international attention from regulators

• Operational privacy management standards
  – Technical standards and architectures for privacy management not yet available

• Relentless Adoption of New Business Models and Infrastructures
  – Social networking
  – Ubiquitous networked applications
  – Internet of Things
  – E-Government
  – Cloud Computing
  – Smart Grid
  – Health IT

• What is Personal Information – Personally Identifiable Information?
Complex Privacy Policy and Regulatory Landscape

• The Privacy Act of 1974 (U.S.)
• Council of Europe Convention 108
• OECD Privacy Guidelines
• UN Guidelines Concerning Personalized Computer Files
• Hong Kong Personal Data (Privacy) Ordinance
• EU Data Protection Directive 95/46/EC
• Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule
• Canadian Standards Association Model Code (incorporated in the Personal Information Protection and Electronic Documents Act [PIPEDA])
• International Labour Organization (ILO) Code of Practice on the Protection of Workers’ Personal Data
• US FTC statement of Fair Information Practice Principles
• US-EU Safe Harbor Privacy Principles
• Ontario Privacy Diagnostic Tool
• Australian Privacy Act – National Privacy Principles
• California Senate Bill 1386, “Security Breach Notification”
• AICPA/CICA Privacy Framework
• Japan Personal Information Protection Act
• APEC (Asia-Pacific Economic Cooperation) Privacy Framework
Global Privacy Principles/Practices
- No Policy Standardization

OECD Guidelines – 1980
- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

Australian Privacy Principles – 2001
- Collection
- Use and Disclosure
- Data Quality
- **Data Security**
- Openness
- Access and Correction
- Identifiers
- Anonymity
- Trans-border Data Flows
- Sensitive Information

APEC Privacy Framework – 2005
- Preventing Harm
- Notice
- Collection Limitation
- Uses of Personal Information
- Choice
- Integrity of Personal Information
- **Security Safeguard**
- Access and Correction
- Accountability

Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)
Yet ...Commonality Among Disparate Principles/Practices

- Accountability
- Notice
- Consent
- Collection Limitation
- Use Limitation
- Disclosure
- Access & Correction
- Security/Safeguards
- Data Quality
- Enforcement
- Openness

- Anonymity
- Data Flow
- Sensitivity

from ISTPA “Analysis of Privacy Principles: An Operational Study” (2007)
Security

• Well-Understood Security Services
  – Confidentiality
  – Data Integrity
  – Availability

• Examples of Standards
  – AES
  – SAML 2.0
  – PCI-DSS
  – ISO 27001/2....etc.

• Rich and Mature Discipline – Cryptography, Controls...
• Many Mechanisms/Technologies/Solutions/Products
Key Security Mechanisms Support Privacy...

- **Identity Lifecycle Management and Compliance**
  - critical to privacy – the correct people should have access to the correct information in a well defined identity system utilizing appropriate role model policies

- **Web access management, federation, Service Oriented Architecture security**
  - Trust among multiple entities to facilitate controlled sharing of information – strengthens security in complex infrastructures

- **Resource Protection**
  - Privileged users are high risk and must be controlled and monitored

- **Data Protection**
  - Data (at rest, in motion) must be monitored for improper leakage

- **Log management**
  - provides the ability to watch what is happening -monitoring is key to maintaining privacy
Privacy Management Challenges:

Cloud Computing
World Economic Forum 2009 Study on Cloud Computing..Deployment

• Economic Benefits
  • Entrepreneurship; create new businesses, jobs
  • Platform for innovation; accelerate innovation
  • Increase IT efficiency and IT flexibility
  • Business/technology leapfrogging opportunities in developing countries

• But...Major Barriers
  • Privacy (63%)
  • Data governance (e.g. data ownership, cross-border data transfer, etc. (56%)
  • Security (50%)

Source: The World Economic Forum - Used with Permission

Addressing security challenges on a global scale

Geneva, 6-7 December 2010
Privacy Management Challenges:

Smart Grid
Smart Grid – Sample Components with Privacy Implications

• Digital information and controls technology
• Dynamic optimization of grid operations and resources with cyber-security
• Deployment of `smart' technologies that optimize the physical operation of appliances and consumer devices
  – for metering, communications concerning grid operations and status, and distribution automation
• Integration of `smart' appliances and consumer devices
• Provision to consumers of timely information and control options
• Two-way communications
• See www.nist.gov/smartgrid

(Source: Energy Independence and Security Act of 2007)
Privacy Management Challenges:

Networked Health IT
Managing Networked PI - Interactive Data Flows

- Non-sequential
- Data subject impacted directly and indirectly after initial data collection

Requestors/Users

Business Application 1, 2... n

Processor/Aggregator 1, 2... n

PI Life Cycle Perspective

Geneva, 6-7 December 2010

Addressing security challenges on a global scale
Challenge:

Making a Reference Model that is PI and Policy–Centric
Managing Multiple Policy Instances
“PI” as Objects - Policies as Objects...
... Managed in Networked “Lifecycle” Context
...with integrated Security Services

- PI Objects
  - PI Policy Objects
    - PI Collection
      - PI Use
        - Aggregation And Linkages
          - PI Use
            - Identity Lifecycle
            - Access
            - Federation
            - Data resource protection
            - Audit
            - Encryption...etc.
Some Privacy Standardization Efforts

• W3C - P3P 1.1 Platform for Privacy Preferences
  Grammar for expressing privacy preferences

• CEN/ISSS Data Protection and Privacy Workshop 2008-2009
  Work Programme
  Best practices management system guide; privacy audit tools

• ISO 29100 (privacy framework)
• ISO 29190 (privacy capability assessment framework)
• ISO 29101 (privacy reference architecture)

• OASIS Cross-Enterprise Security and Privacy Authorization
  (XSPA) Technical Committee
  Exchange privacy policies, consent directives, and authorizations
  within/between healthcare organizations
What is Needed

• An Operational Model supporting:
  – the assured, proper, and consistent collection, processing, communication, use and disposition of personal information (PI) throughout its life cycle
  – consistent with data protection principles, policy requirements, and the preferences of the individual

• Proper and consistent apply throughout the PI life cycle

• Applicable to all actors, systems, and networks that “touch” the information

• An abstract model enabling networked, full lifecycle privacy management
Privacy Management Reference Model Services

• Core Policy Services
  – Agreement - agreements, options, permissions
  – Control – policies – data management

• Presentation and Lifecycle Services
  – Interaction - manages data/preferences/notice
  – Agent - software that carries out processes
  – Usage - data use, aggregation, anonymization
  – Access - individual review/updates to PI

• Privacy Assurance Services
  – Certification - credentials, trusted processes
  – Audit - independent, verifiable accountability
  – Validation - checks accuracy of PI
  – Enforcement - including redress for violations
Making Privacy Operational

PI Touch Point

- Each Touch Point node configured with operational stack
- Privacy Policy is an input “parameter” to Control
- Agent is the Touch Point programming persona
- PIC contains PI and usage agreements

Interaction
Agreement
Control

PI, Preferences & PIC Repository

Access
Usage

PI Container (PIC)

Assurance Services
- Validation
- Certification
- Audit
- Enforcement

Security Foundation

Geneva, 6-7 December 2010
Addressing security challenges on a global scale
Privacy SERVICES

Any two touch points in the PI life cycle

Agent

Interaction
Agreement
Control

PI, Preferences & PIC Repository

Agent

Interaction
Agreement
Control

PI Container (PIC)

PI Container (PIC)

Assurance Services

Validation
Certification
Audit
Enforcement

Security Foundation

Addressing security challenges on a global scale

Geneva, 6-7 December 2010
Support for Networked-Interactive Data Flows

Individual

Requestors/Users

Business Application 1, 2... n

Processor/Aggregator 1, 2... n

PI Life Cycle: PMRM per Touch Point

Geneva, 6-7 December 2010

Addressing security challenges on a global scale
Syntax for each Service: Functions

- **DEFINE [SVC]** operational requirements
- **SELECT [SVC]** (input, process, and output) data and parameters
- **INPUT [SVC]** data and parameter values in accordance with Select
- **PROCESS [SVC]** data and parameter values within Functions
- **OUTPUT [SVC]** data, parameter values, and actions
- **LINK [SVC]** to other (named) Services
- **SECURE [SVC]** with the appropriate security functions

- Each USE CASE invokes a sequence of Service “calls”

- Each Service call executes a sequence of Functions (drawn from these seven Functions)

**TWO EXAMPLES**
Where Does the Reference Model Fit?

Addressing security challenges on a global scale

Geneva, 6-7 December 2010
Current PMRM Activities

- OASIS Privacy Management Reference Model (PMRM) Technical Committee
  - First meeting September 8, 2010
  - Deliverables include
    - the Reference Model
    - use cases utilizing the PMRM
    - formal methodology for expressing use cases
    - profiles of the PMRM applied to selected specific environments such as Cloud Computing
    - linkages to security services
- Seek liaison relationships to test the Reference Model against use cases and privacy scenarios
- Coordinate as much as possible with other standards efforts
- Charter includes specific reference to international standards bodies such as ITU and ISO
Questions?

John Sabo
john.t.sabo@ca.com

Contributed PMRM available at www.oasis-open.org