Making Privacy Operational

Introduction to the Privacy Management Reference Model

John Sabo

Director, Global Government relations

CA, Inc. and President, ISTPA

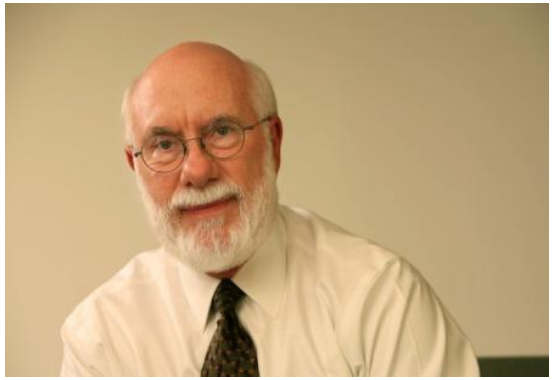
john.t.sabo@ca.com

Michael Willett

President, WillettWorks Technology

and Board member, ISTPA

mwillett@nc.rr.com



John Sabo is Director, Global Government Relations for CA, Inc., serves as an industry expert in the use of security and privacy technologies in trusted infrastructures.

He is as an appointed member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee, and is a past member of National Institute of Standards and Technology Information Security and Privacy Advisory Board (ISPAB). He is a board member and President of the non-profit International Security Trust and Privacy Alliance (ISTPA) and is a member of the OASIS IDtrust Member Section Steering Committee.

John is active in information sharing, cyber-security and critical infrastructure protection committees and organizations. He is a board member and past President of the Information Technology-Information Sharing and Analysis Center (IT-ISAC); member of the IT-Sector Coordinating Council; and Immediate Past Chair of the ISAC Council.

Dr. Michael Willett received his BS degree from the US Air Force Academy (Top Secret clearance) and his Masters and PhD in mathematics from NC State University. After a career as a university professor of mathematics and computer science, Dr. Willett joined IBM as a design architect, moving into IBM's Cryptography Competency Center. Later, Dr. Willett joined Fiderus, a security and privacy consulting practice, subsequently accepting a position with Wave Systems. Recently, Dr. Willett was a Senior Director in Seagate Research, focusing on security functionality on hard drives, including self-encryption, related standardization, product rollout, patent development, and partner liaison. Currently, Dr. Willett provides consultation for marketing storage-based security. Dr. Willett also chairs the Privacy Management Reference Model Project of the ISTPA, which developed an operational reference model for implementing privacy requirements.

Webinar Objectives

- Introduce the Privacy Management Reference Model (PMRM) and proposed OASIS Technical Committee

- Solicit companies, agencies and individuals as “proposers” to establish the PMRM TC
  - Both current OASIS members and new members
  - Foster interest in use-case development

- Start a discussion group to generate interest, questions and prepare for the new TC

Why Do We Need a Privacy Management Reference Model?

John Sabo

First - What is Data Privacy?
-expressed as Principles/Practices

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

- *Anonymity*
- *Data Flow*
- *Sensitivity*

Global Privacy Principles/Practices - similarities...but no Standardization

from ISTPA "Analysis of Privacy Principles: An Operational Study" (2007)

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)

And yet…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 devices
  - E-Government
  - Cloud Computing
  - Health IT
  - Smart Grid

Privacy Management Challenges:

Cloud Computing

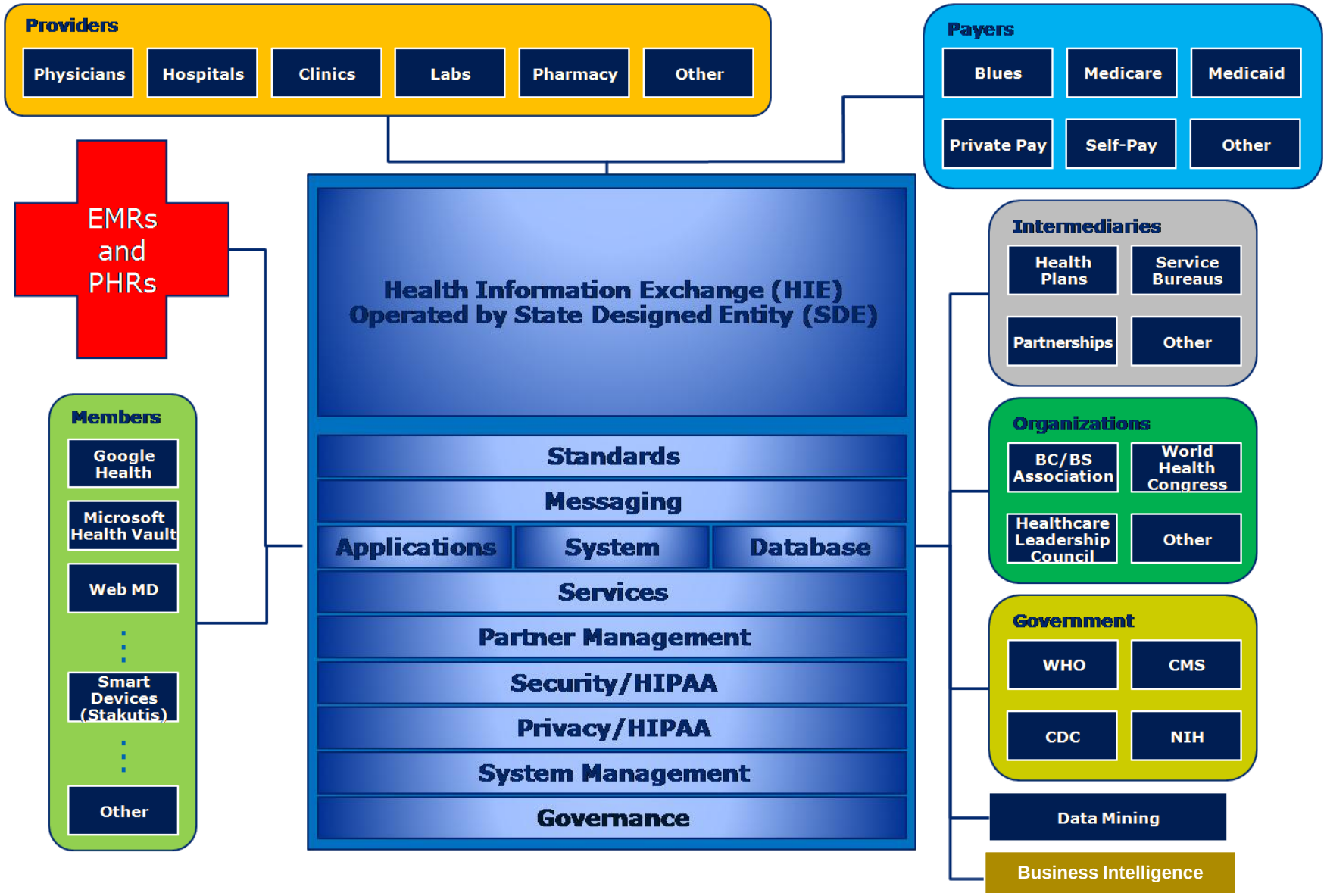
World Economic Forum 2009 Study on Cloud Computing..Deployment

- 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

Privacy Management Challenges:

the emerging networked Health IT environment



Health Information Exchange Functional and Roles Diagram

Privacy Management Challenges:

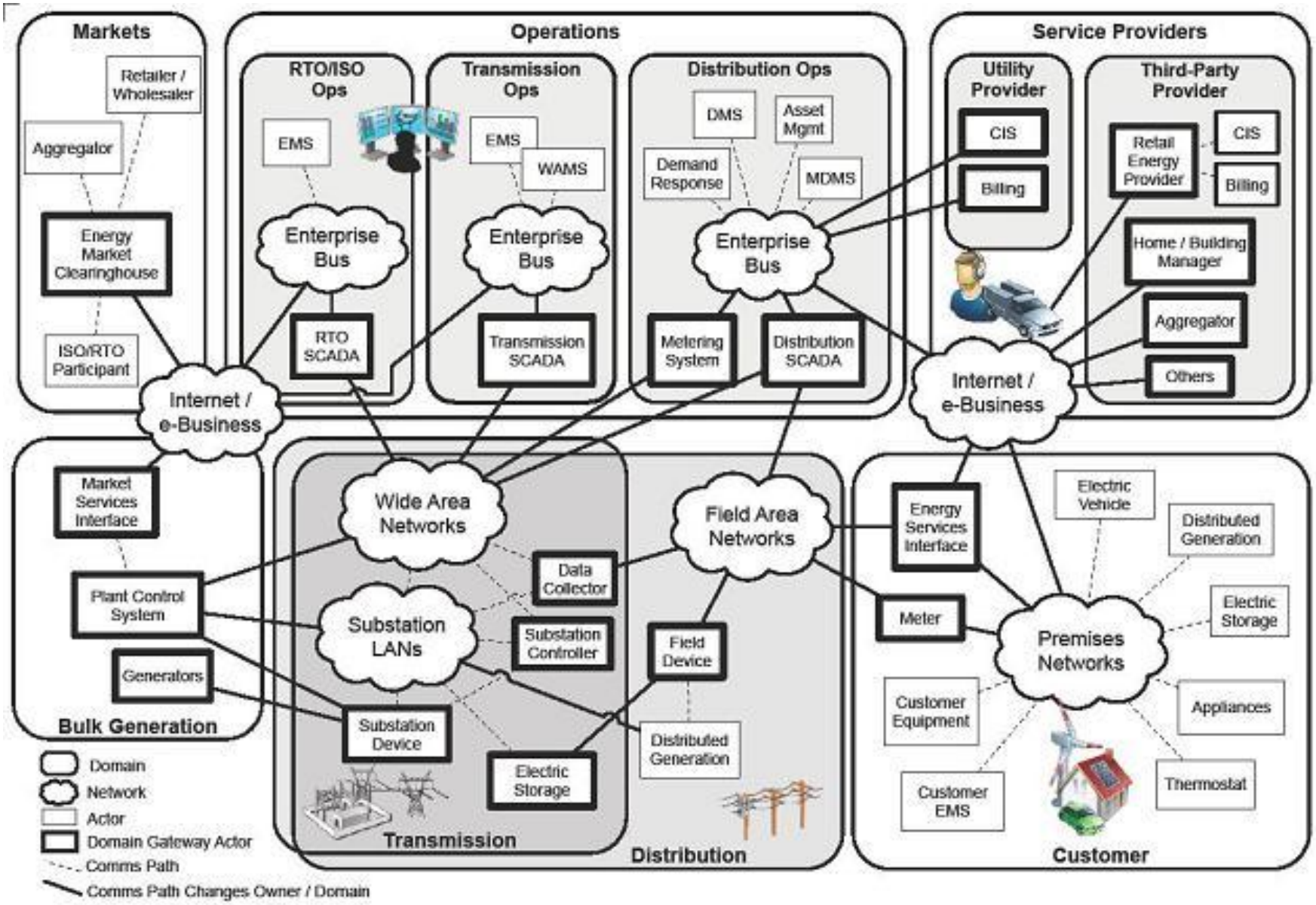
the new Smart Grid

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)

NIST Smart Grid Conceptual Model



Source: 27 NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0

Addressing Lifecycle Privacy Management

ISTPA

- The International Security, Trust and Privacy Alliance (ISTPA), founded in 1999, is a global alliance of companies, institutions and technology providers working together to clarify and resolve existing and evolving issues related to security, trust, and privacy

- ISTPA's focus is on the protection and management of personal information (PI) – www.istpa.org

ISTPA

Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

ISTPA's Perspective on Privacy

- Operational, Technical, Architectural Focus
  - Based on legal, policy and business process/control drivers
  - Privacy management with support for lifecycle requirements
  - "Reference Model" for system designers
- "Analysis of Privacy Principles: An Operational Study" (2007)
  - 14 Composite Principles
- Privacy Management Reference Model V2.0 (2009)
  - Major revision of Privacy Framework v1.1 (2002)
  - Supports the full "lifecycle" of Personal Information
  - Converts privacy requirements to operational Services

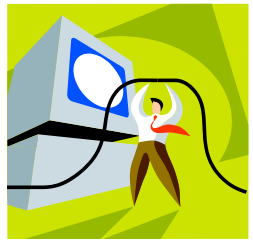
Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

Managing Networked-Interactive Data Flows

Requestors/Users

Time

Requestors/Users ..n …



PI

PI

PI

PI

Individual

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

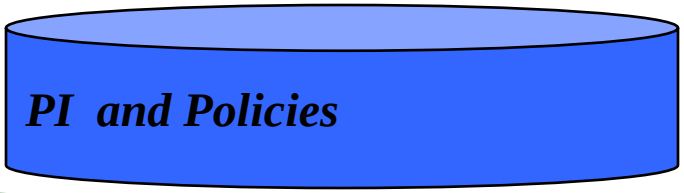
Business Application 1, 2… n

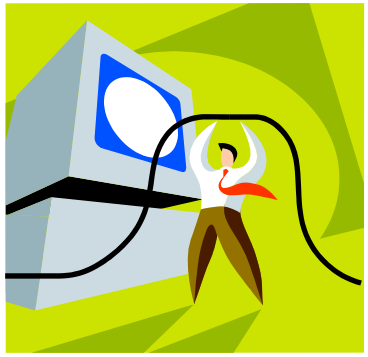
Processor/Aggregator 1, 2…n

PI Life Cycle Perspective

Challenge:

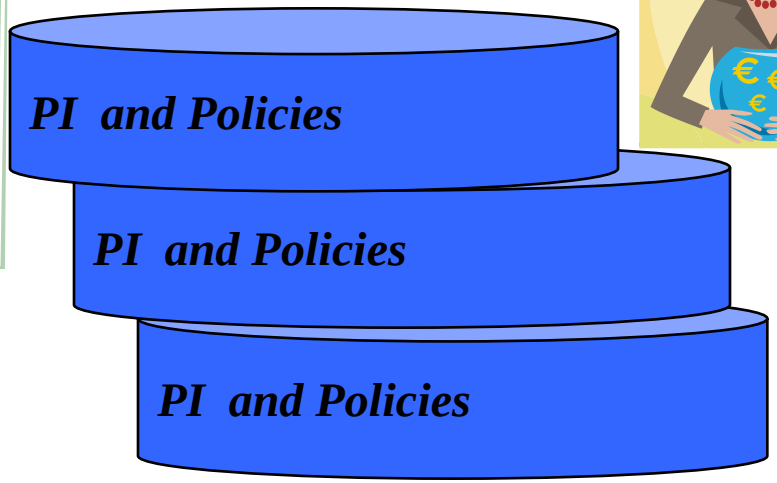
Making the New Reference Model PI and Policy–Centric

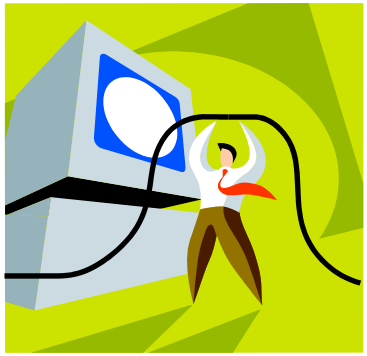




Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

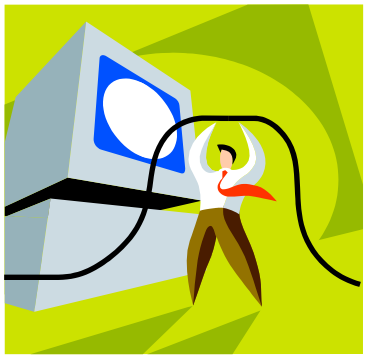
Managing Multiple Policy Instances

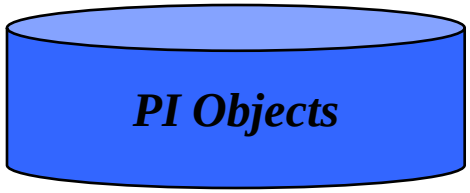


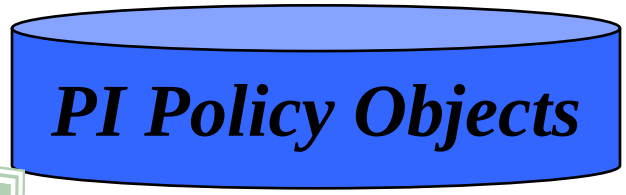


Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

"PI" as Objects - Policies as Objects…



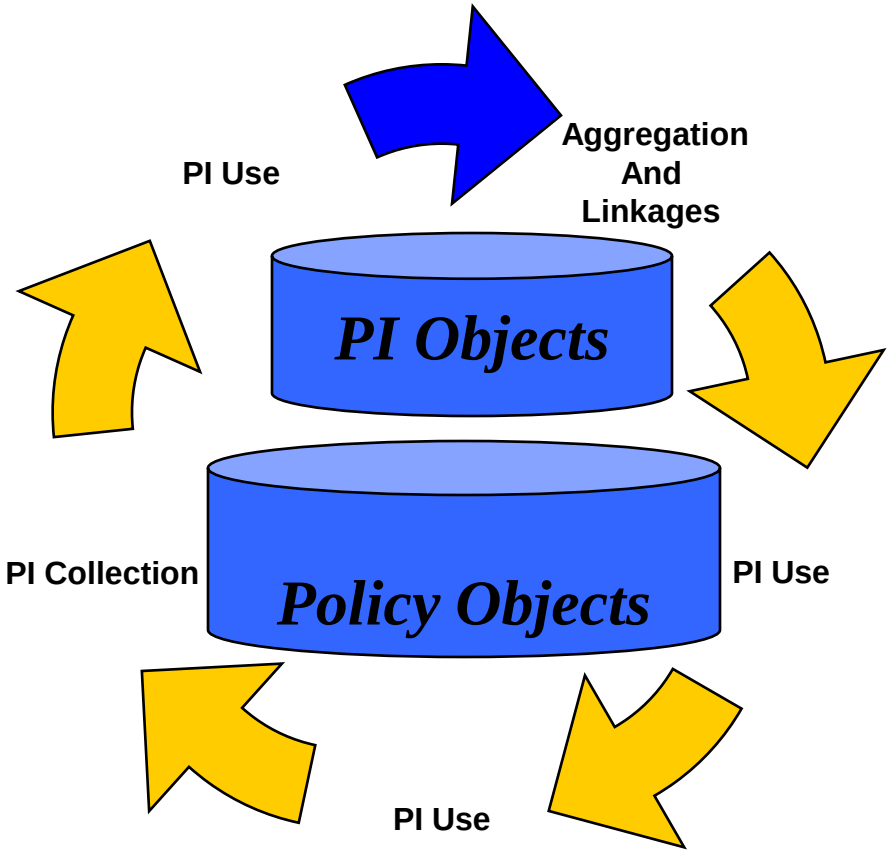




System Design perspective

Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

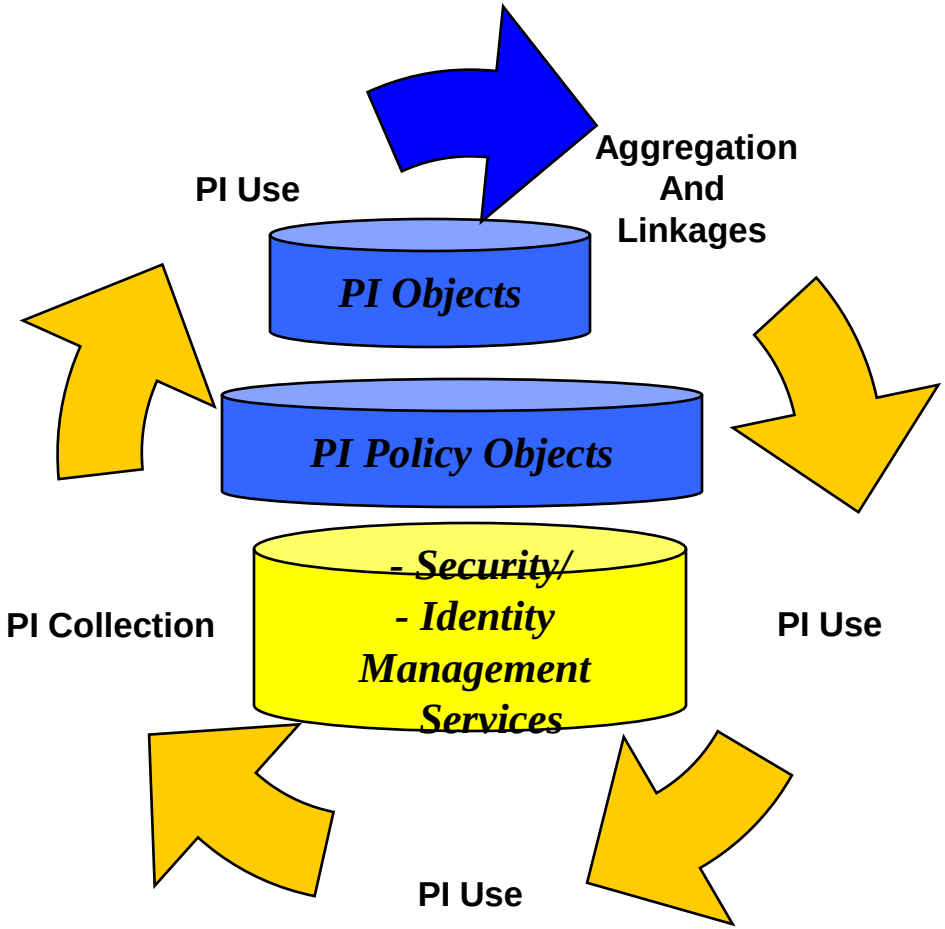
… Managed in Networked "Lifecycle" Context



System Design perspective

Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

...with integrated Security Services



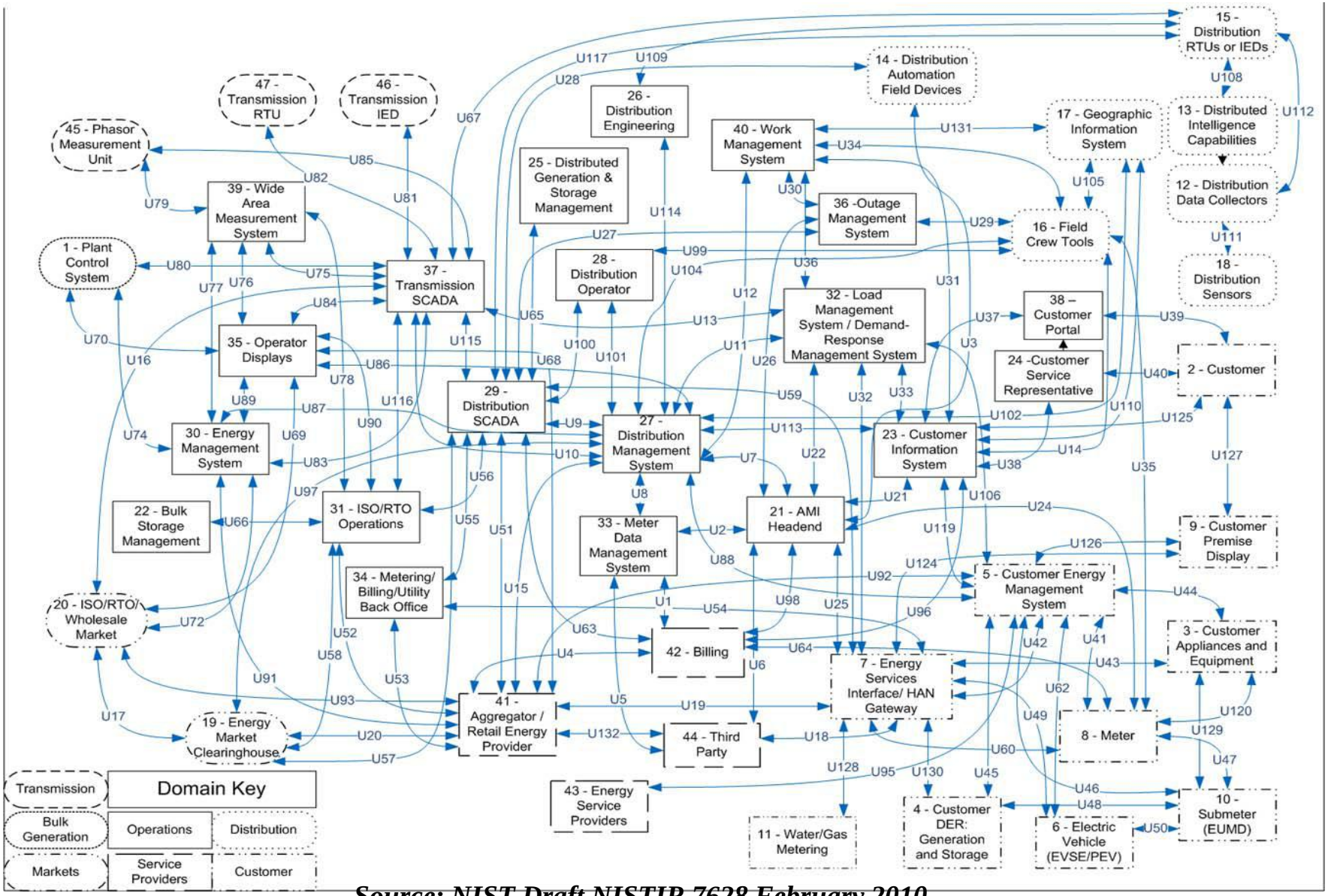
System Design perspective

Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

...only a standards-based, structured model will enable us to implement, manage and ensure compliance with privacy policies in existing and emerging infrastructures

...such as this smart grid logical architecture...

Unified Logical Architecture for the Smart Grid



Source: NIST Draft NISTIR 7628 February 2010

Toward Operational *Privacy Management*

Michael Willett

Privacy Standardization

- *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

- *OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) Technical Committee*

  Exchange privacy policies, consent directives, and authorizations within/between healthcare organizations

Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

What else is missing?

ANSWER: A LOT!

- **Operational view: information privacy *is 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**
  - apply to all actors, systems, and networks that "touch" the information

Need an abstract model enabling full life cycle privacy management

Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

“Framework” (2002) to “Reference Model” (2009)

- From a policy perspective, ISTPA received pushback on use of the term “framework” in 2002 document
- Framework v1.1 services were validated, but lacked reference to networked, asynchronous lifecycle
- Need to support use cases where PI is disassociated from the data collector and the individual’s control
  - Information life cycle beyond the collector
  - Policy changes in the future
- Improved understanding of Service-to-Service relationships; formalized syntax for modeling/simulation
- Tested against composite privacy principles derived globally

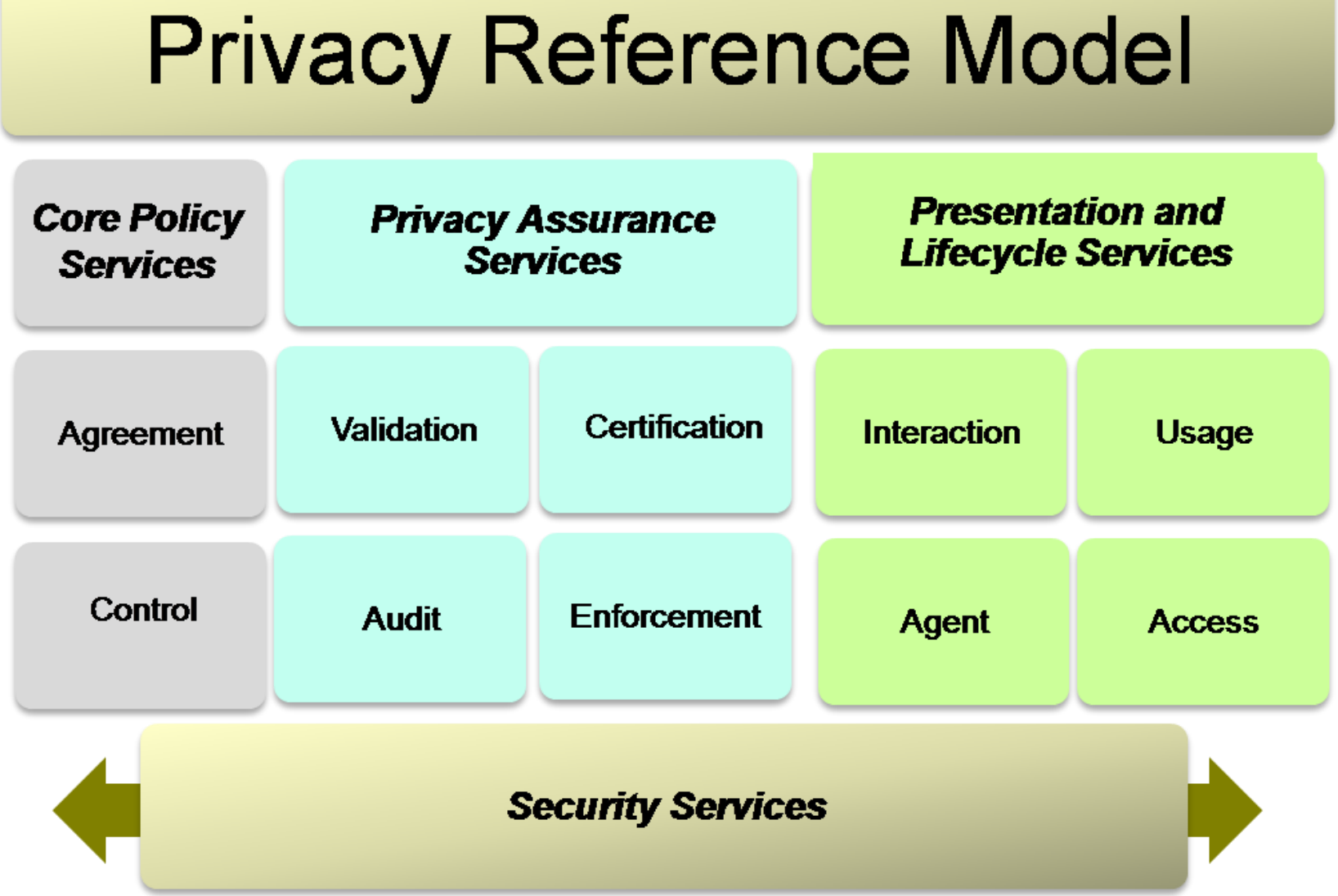
Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

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

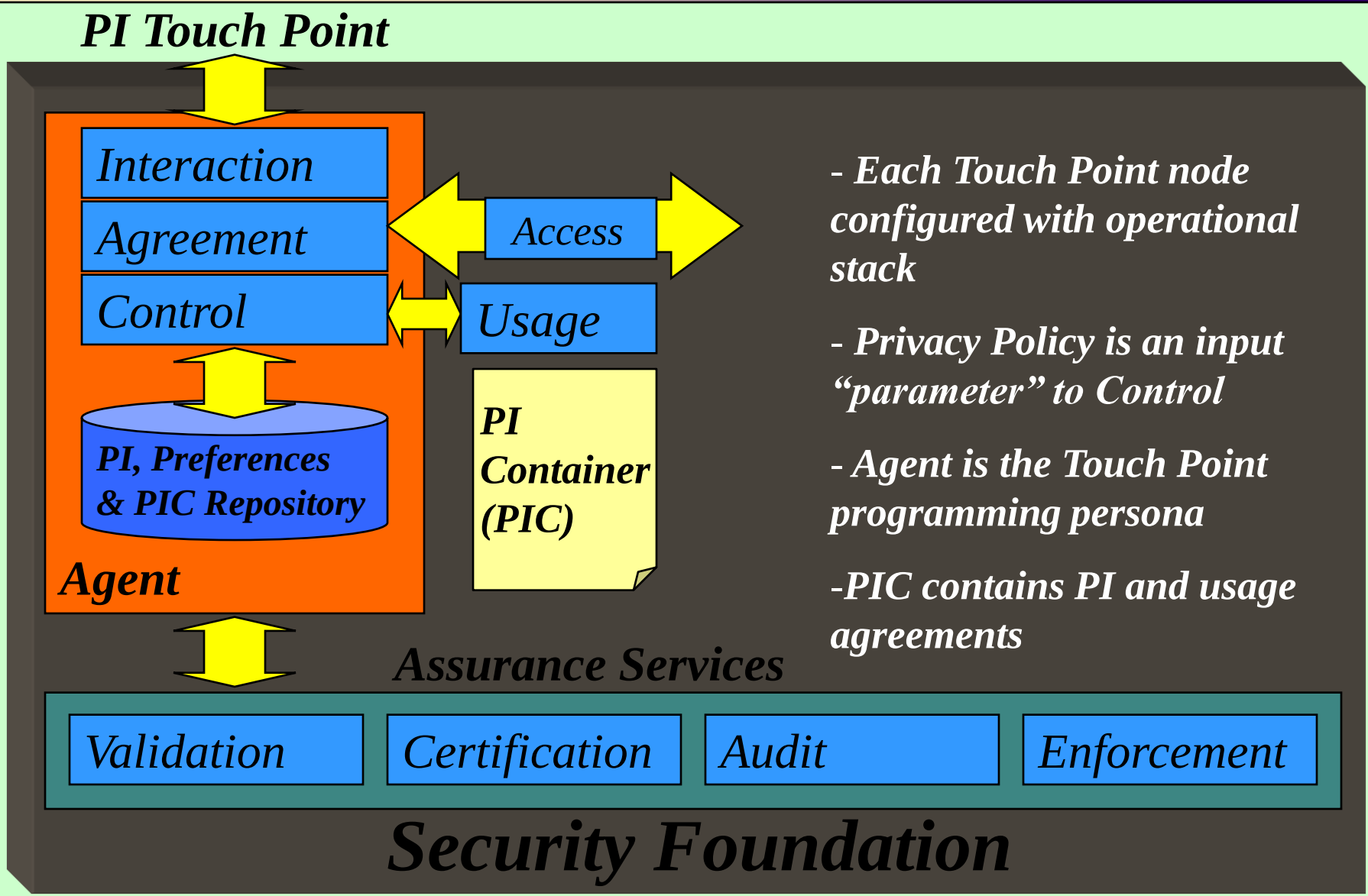
Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

Privacy Reference Model



Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

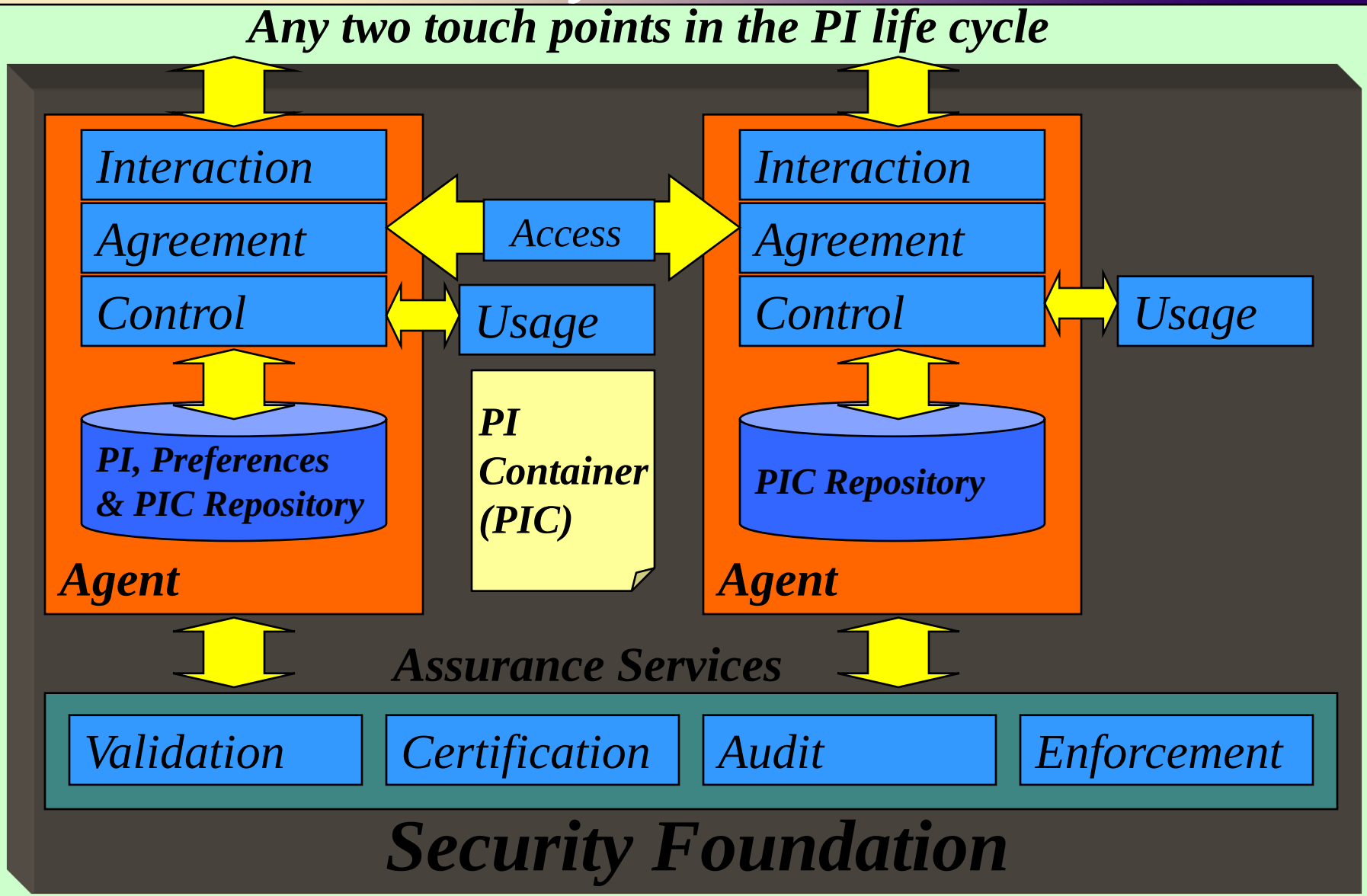
Making Privacy Operational



Legal, Regulatory, and Policy Context

Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

Privacy SERVICES



Legal, Regulatory, and Policy Context

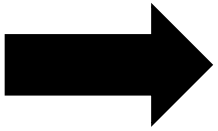
Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

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 

Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

Agreement

The Agreement Service provides information to individuals regarding what PI is collected, for what purposes it will be used, other policies and options associated with the collection and use, and can result in consent, denial or an agreement among the parties. The Agreement Service also enables any set of parties (individuals, processing entities) to define agreements related to policies, use and disposition associated with the PI at points throughout the PI lifecycle.

Control

The Control Service encompasses the functions that work together to ensure that PI governed by fair information practices/principles is managed in accordance with prescribed privacy policies and controls. These functions are established, maintained and manipulated by a processing entity.

Example: Agreement Functions

DEFINE Agreement requirements

Establish objectives and scope for the Agreement service

SELECT Agreement parameters for Input, Process, and Output

INPUT Agreement of PI definition

INPUT Agreement for additional permissions

Exchange initial parameters related to a potential agreement between parties

PROCESS Agreement parameters

PROCESS Agreement exchange

PROCESS Agreement interchange

Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

… Example: Agreement Functions

OUTPUT Agreement results

Output the consent, denial or an agreement among the parties

LINK Agreement to another Service

Connect Agreement with another Service and pass outputs and other parameters between

Agreement and that Service, as appropriate

SECURE Agreement

Invoke security controls in support of Agreement functions, as appropriate

Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

(Another) Example: Control Functions

DEFINE Control requirements

Establish objectives/scope; document rules and standards

SELECT Control parameters for Input, Process, and Output

INPUT Control association to PI usage

INPUT Control rules from Policy

PROCESS Control configuration

PROCESS Control management

PROCESS Control of PI input/output

Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

… Example: Control Functions

OUTPUT Control interaction with internal parties or systems

OUTPUT Control interaction with external parties or systems

LINK Control to another Service

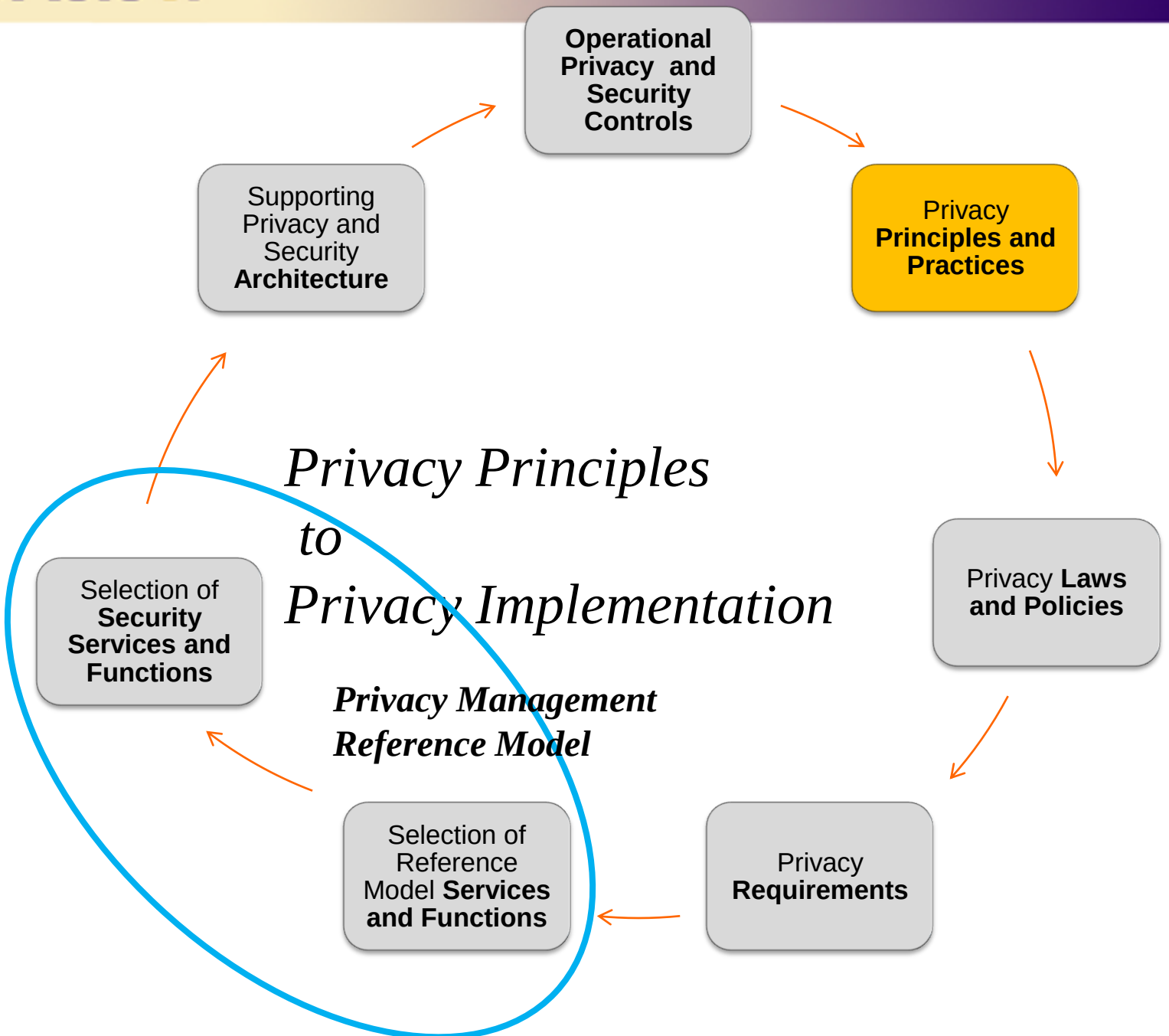
Connect Control with another Service and pass outputs and other parameters between

Control and that Service, as appropriate

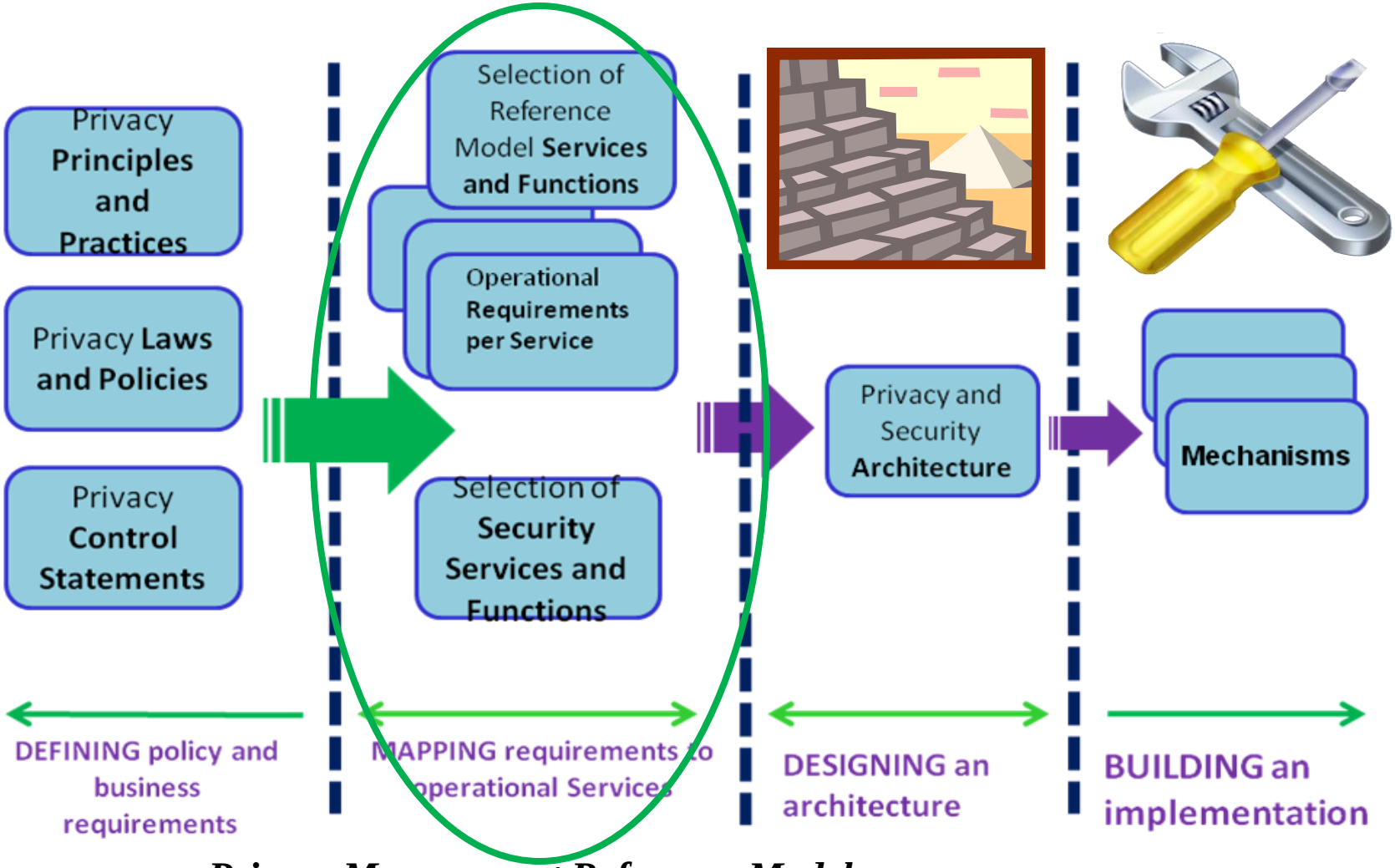
SECURE Control

Invoke security controls in support of Control functions, as appropriate

Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)


Operational Privacy and Security Controls
Privacy Principles and Practices
Privacy Laws and Policies
Privacy Requirements
Selection of Reference Model Services and Functions
Selection of Security Services and Functions
Supporting Privacy and Security Architecture
Privacy Principles to Privacy Implementation
Privacy Management Reference Model

Where Does the Reference Model Fit?

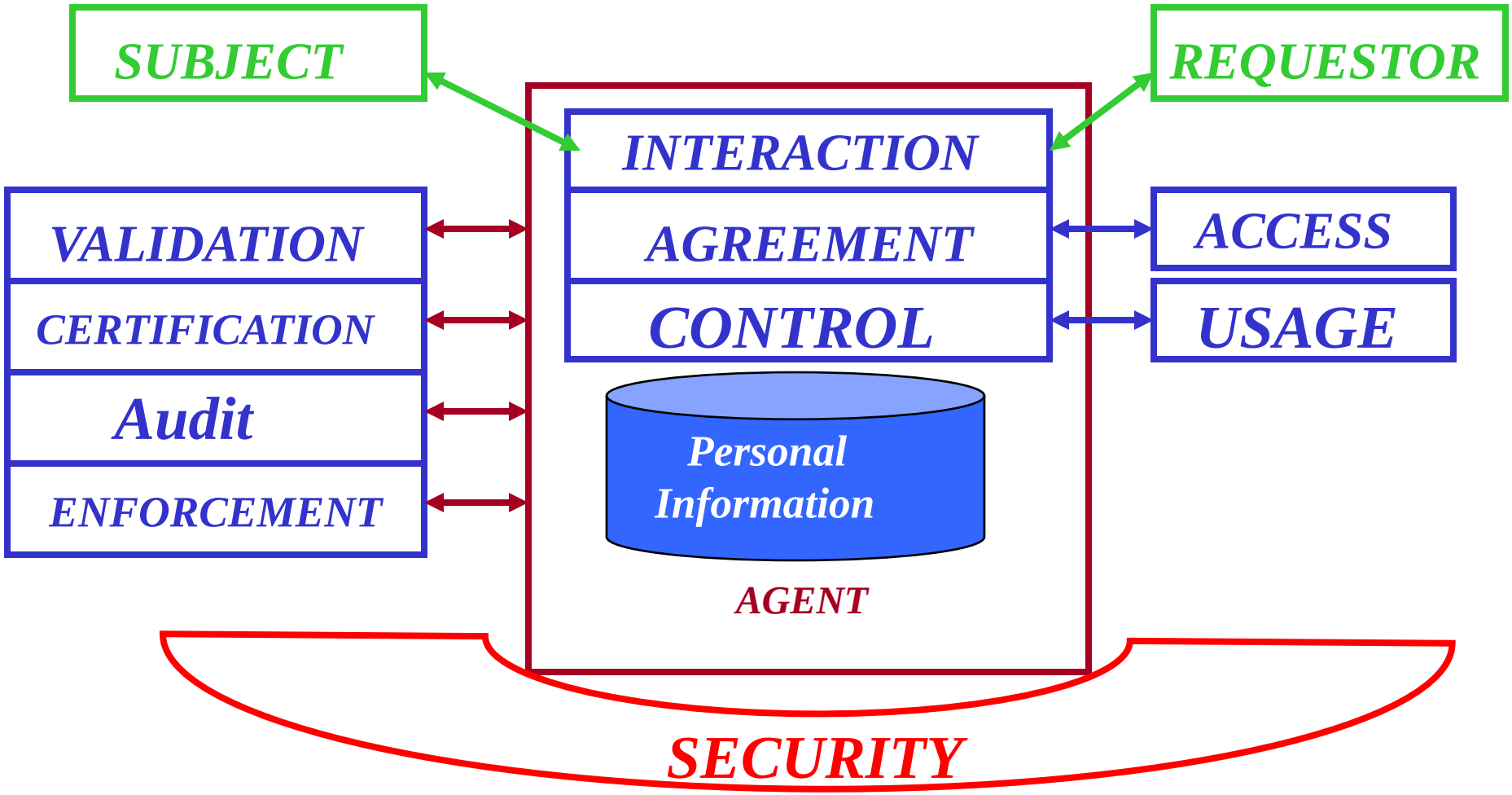


Privacy Management Reference Model

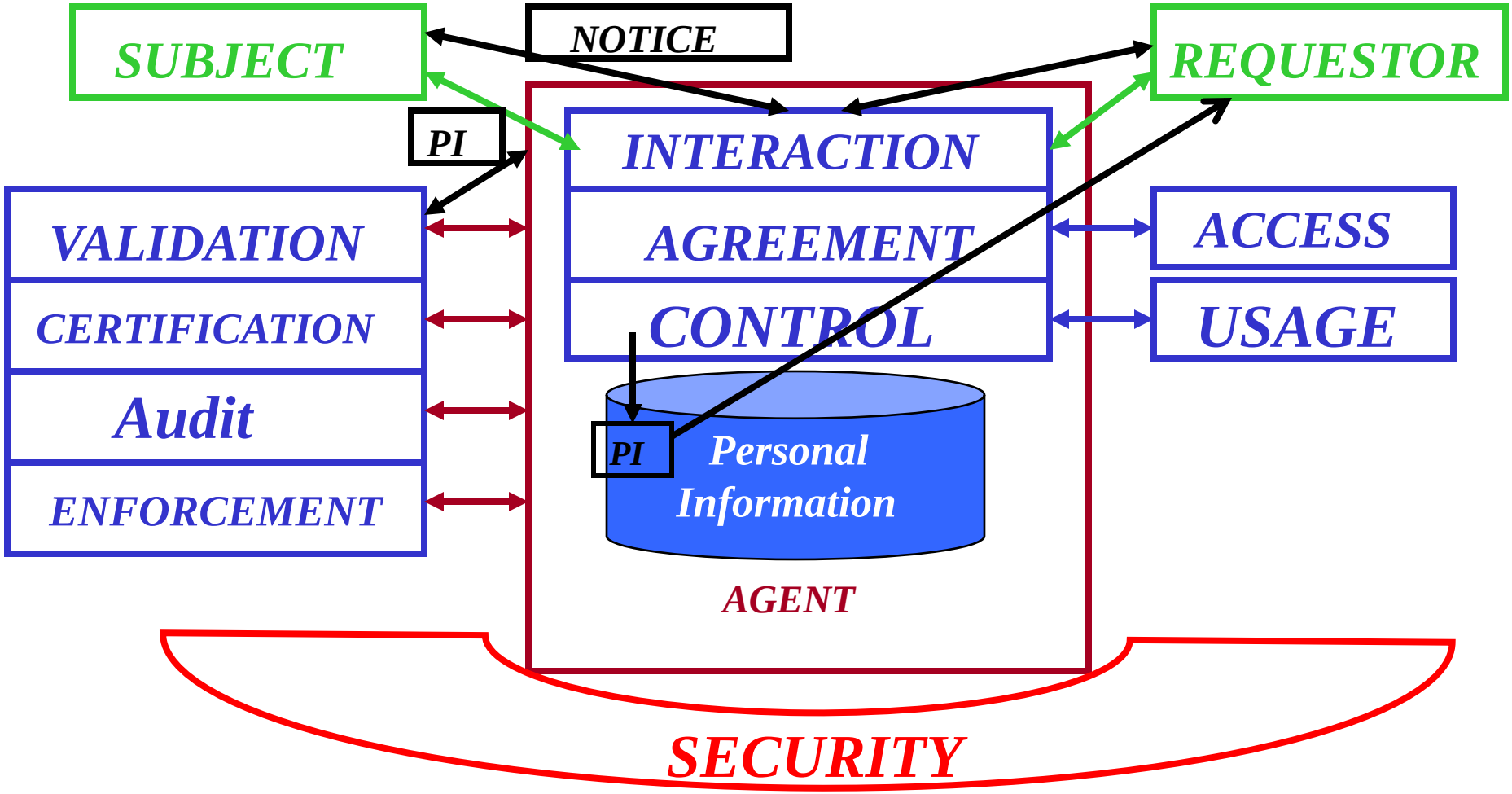
Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

Simple Use Case

Employer application like Payroll that requests certain PI from an employee…



Employer (Requestor) AGENT and INTERACTION: a NOTICE of the purpose/use of requested PI is presented to the SUBJECT. The PI, together with the permissible purpose/use, is submitted for VALIDATION, then stored in the PI database by CONTROL and transferred to REQUESTOR.



Next Steps

- Proposing an OASIS Privacy Management Reference Model (PMRM) Technical Committee
  - Soliciting initial “proposers” (e.g., ISTPA, NIST, ABA, CA, others)
  - Drafting the TC Charter
  - Planning the first TC meeting (probably in Washington, DC)
- Looking for partners to host workshops to test the Reference Model against use cases and privacy scenarios
- TC Objectives: Formally develop the PMRM, define functions, develop relevant use cases, identify business process and technical mechanisms to support the PMRM and establish the PMRM as an industry standard
- Smart Grid Coordination with OASIS Blue Member Section

Copyright © 1999-2010 International Security Trust and Privacy Alliance (ISTPA)

Questions?

John Sabo

john.t.sabo@ca.com

Michael Willett

mwillett@nc.rr.com

Dee Schur (OASIS)

dee.schur@oasis-open.org

PMRM available at www.istpa.org