ISTPA
INTERNATIONAL SECURITY TRUST & PRIVACY ALLIANCE

Security Privacy Trust

ISTPA Master ToolSet for Privacy

Michael Willett (Seagate)

Framework Committee Chair

3 Nov 2006

CACR/Toronto

ISTPA Privacy Framework: Revision and Utilization

- Analyzed: NON-operational privacy principles and practices
- Result = Framework: 10 Operational Services, derived and tested
- Submitted to ISO/JTC1 as a PAS (through ISSEA)
- Data Commissioners recommend more exposure and application
- ISTPA: Three Projects = Revision, ToolSet, Security
- Revision: Analyze worldwide principles/practices/legislation
- Revision: Systematic restructure of Service functions
- ToolSet: Repeatable process to morph privacy reqs to Framework
- Security: (w/ISSEA) Identify security requirements per Service

ToolSet: What is it?

- ToolSet = “Applying” the Framework to a privacy management problem
- Needed to help guide the “system design” for privacy management
- Multiple choices for ToolSet method
- ToolSet lends itself to automation and modeling

ToolSet Process: Objectives

-Given: Set of Privacy REQUIREMENTS (P-REQ)

- P-REQ = practices, principles, regulations, checklists, etc

- P-REQ typically NOT operational (HOW to implement?)

-Framework Services ARE focused on implementation

-ToolSet Process: Morph P-REQs into Services

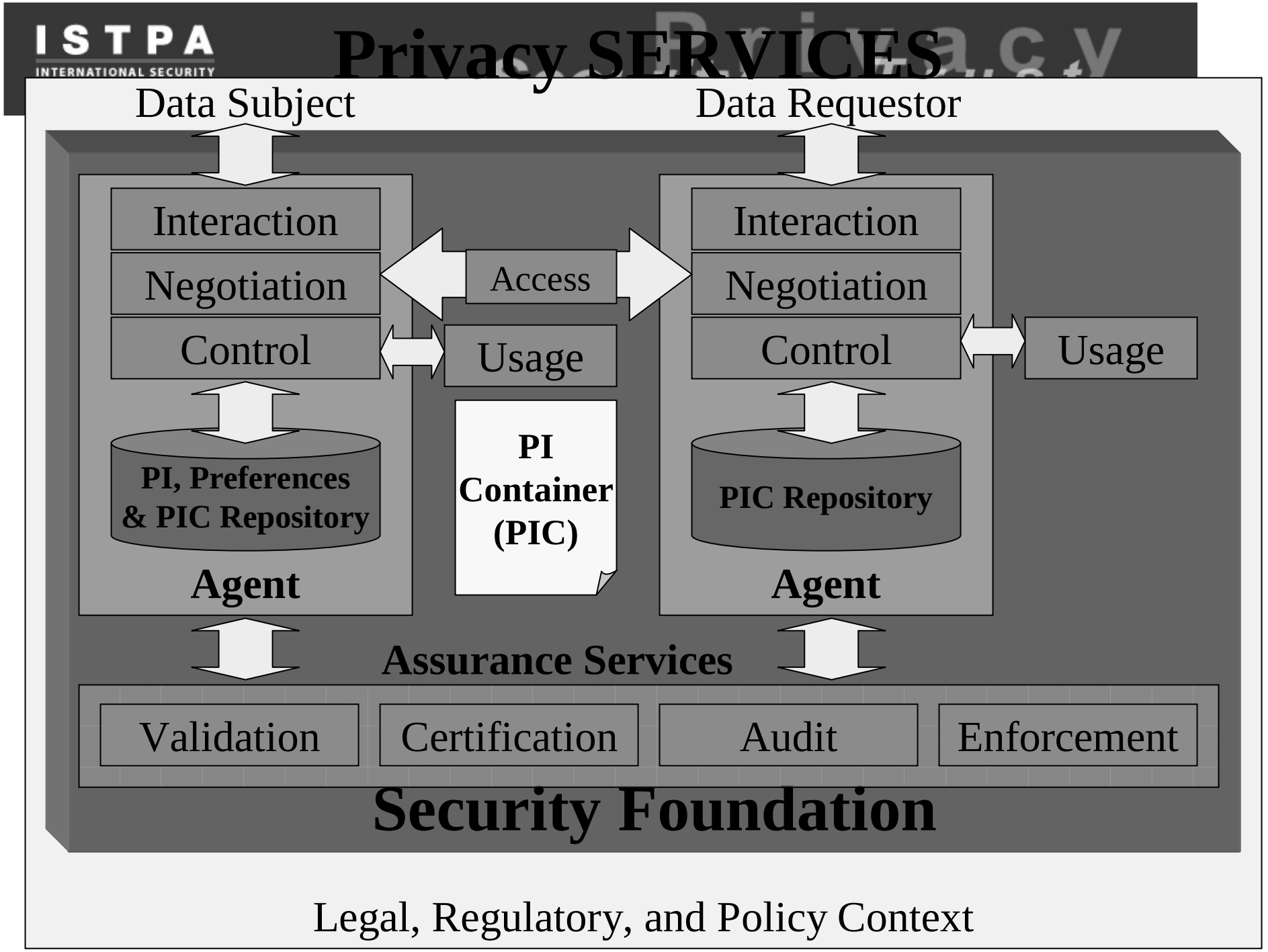
- ToolSet amenable to automation

- Test ToolSet Process against varied P-REQ sets

Privacy Services

- ☑ Interaction
- ☑ Agent
- ☑ Validation
- ☑ Negotiation
- ☑ Enforcement
- ☑ Control
- ☑ Audit (Log)
- ☑ Certification
- ☑ Usage
- ☑ Access

Service / Capability	Description
Audit	Handles the recording and maintenance of events in any service to capture the data that is necessary to ensure compliance with the terms and policies of an agreement and any applicable regulations.
Certification	Manages and validates the credentials of any party or process involved in processing of a PI transaction.
Control	Functions as "repository gatekeeper" to ensure that access to PI that is stored by a data collection entity complies with the terms and policies of an agreement and any applicable regulations.
Enforcement	Handles redress when a data collection entity is not in conformance with the terms and policies of an agreement and any applicable regulations.
Interaction	Presents proposed agreements from a data collection entity to the data subject; receives the subject's personal information, preferences, and actions; confirms actions; manages movement of data into and out of the Framework. To the extent the data subject is represented by an agent, this service comprises the interface to the agent.
Negotiation	Handles arbitration of a proposal between a data collection entity and a data subject. Successful negotiation results in an agreement. Humans, agents, or any combination, can handle negotiation.
Validation	Checks for accuracy of PI at any point in its life cycle.
Access	A capability that allows the data subject to both access the individual's PI that is held by a data collection entity, and to correct or update it as necessary.
Agent	A software capability that acts on behalf of a data subject or a requestor. The Agent Capability engages with one or more of the other services defined in this Framework. Agent can also refer to the human data subject in the case of a manual process.
Usage	Functions as "processing monitor" to ensure that active use of PI complies with the terms and policies of an agreement and any applicable regulations. Such uses may include transfer, derivation, aggregation, pseudo-anonymization, linking, and inference of data.


ISTPA
INTERNATIONAL SECURITY
Privacy SERVICES
Data Subject
Data Requestor
Interaction
Negotiation
Control
Access
Usage
Interaction
Negotiation
Control
Usage
PI, Preferences & PIC Repository
PI Container (PIC)
PIC Repository
Agent
Agent
Assurance Services
Validation
Certification
Audit
Enforcement
Security Foundation
Legal, Regulatory, and Policy Context

Alternative ToolSet Methodologies Considered

1) Put "Do you...." in front of the Services, making the Service into a question (rather light approach).

2) Itemize the Mechanisms under each Service; that is, reduce each Function statement under each Service to a set of specific Mechanisms, in which specific technologies are called out (reduces Mechanism flexibility)

3) Directed Q/A (logic tree), culminating in one of three "buckets" of actions:

- **Policy**
- **Process**
- **Tools (here the Framework Function statements would appear)**

4) Profile = template for Q/As

5) Gap analysis (no Implementation insight)

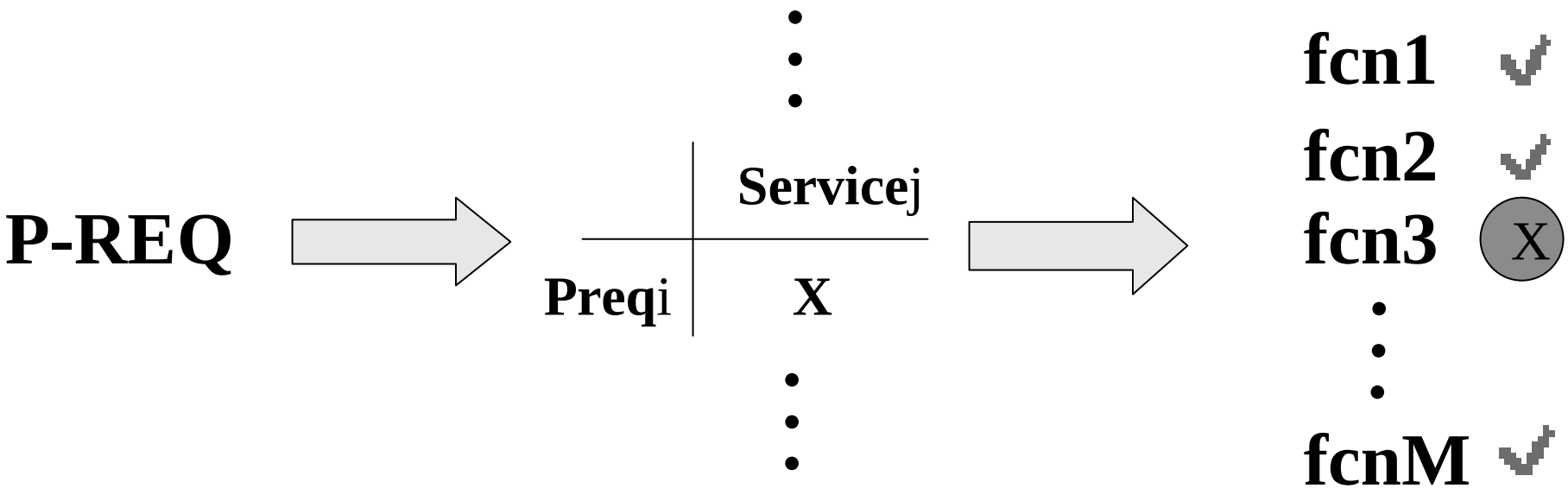
6) Detailed Checklist (not operational)

P-REQ = / Preq1 / Preq2 / … / PreqN/ (decomposition)

	Framework SERVICES			
Preq1		X		X
Preq2	X		X	
•				
•				
•				
PreqN		X			X

Select each Framework SERVICE implicated in Preqi

Further Decomposition to SERVICE Functions



Per Servicej, select specific functions implicated in Preqi (✓)

Successive Decomposition of P-REQs to Services to Functions

Services

Preq

	servicej
Preqi	X

Functions

Atomic Decomposition allows for more objective analysis per step

In addition to Function, a PROCESS can be recommended

(Partial) Example from the Compendium White Paper

	Audit (log)	Certification	Control	Enforcement	Interaction	Negotiation	Validation	Access	Agent	Usage
Accountability	X	X	X	X					X	
Notice					X				X	
Consent		X			X	X		X	X	
Collection Limitation	X				X	X			X	
Use Limitation	X		X		X	X			X	X
Disclosure		X			X	X		X	X	
Access & Correction		X			X	X		X	X	
Security Safeguards	X	X	X					X	X	
Data Quality		X	X				X			
Enforcement	X			X						
Openness					X	X			X	X
Anonymity		X		X		X				
Data Flow					X	X		X	X	X
Sensitivity	X				X	X			X	X

Example: Based on the Ontario Privacy Diagnostic Tool

Accountability

Identifying Purposes

Consent

Limiting Collection

Limiting Use, Disclosure and Retention

Accuracy

Safeguards

Openness

Individual Access

Challenging Compliance

Each Principle is subdivided into more atomic Actions and Best Practices

= P-REQs

Example: "Individual Access" =6 YES/NO Questions and 3 BEST PRACTICES

"Upon request, you tell individuals if you have personal information about them and allow them access to that data, except in limited circumstances" =

1) Upon request

2) tell individuals if you have personal information about them

3) allow them access to that data

4) except in limited circumstances

Services = ….. CERTIFICATION …….

Preqi:

UPON REQUEST:

Process	**Establish system to verify that request is legitimate**
Function i	**Select authentication technique to validate identity credentials**

ToolSet Process: Next Steps

-Successive reduction ("lensing") from P-REQs to Function lists

-Subset (labeled) function list per Service

-Use Function Lists to imply a "System Design"

- OPEN: Synthesize an operational implementation

- Experiment with additional P-REQ lists

- Automation Tool to assist in reduction

-New (labeled) functions added to Service list per experience