ISTPA Privacy Framework

Michael Willett (Seagate)

Framework Committee Chair

3 Nov 2006

CACR/Toronto

HISTORY

Privacy: proper handling and *use* of personal information (PI) throughout its life cycle, consistent with the preferences of the subject

- Privacy Principles/Practices/Legislation NOT Operational

- Wanted a Privacy Management IMPLEMENTATION Framework

- Examined Representative Privacy Practices, for Insight

- Derived the 10 Privacy Framework SERVICES (ad hoc approach)

- Each Service = set of detailed FUNCTIONS

- Services Inter-Connect

Fair Information Practices

Notice and Awareness
Choice and Consent
Individual Access
Information Quality and Integrity
Update and Correction
Enforcement and Recourse

Life Cycle Management of PI

Requestor /Receiver

Touch Points

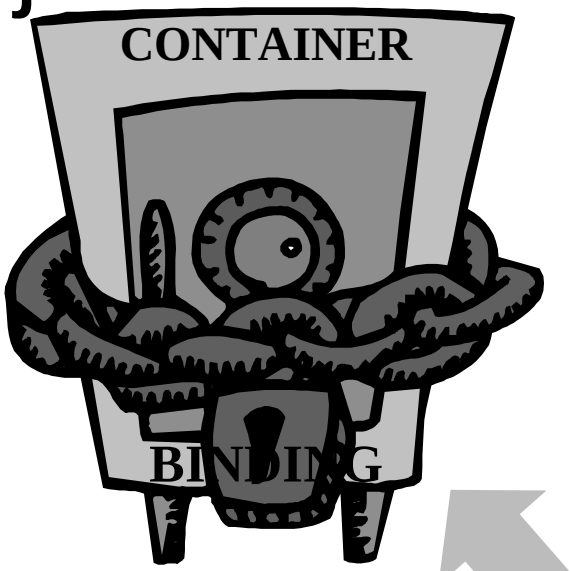
Source/Subject

Intermediary/ Requestor

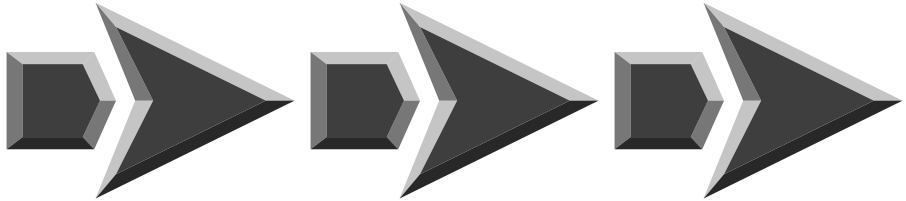
Repository/Custodian

PI Touch Point Structure

Subject "Permission" Bound to PI

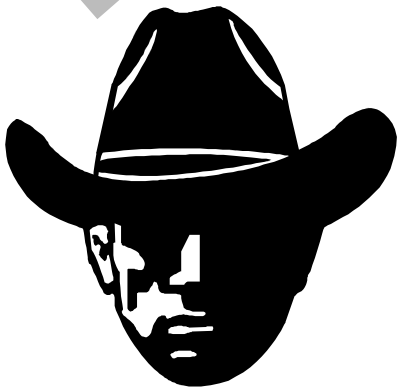


LIFE



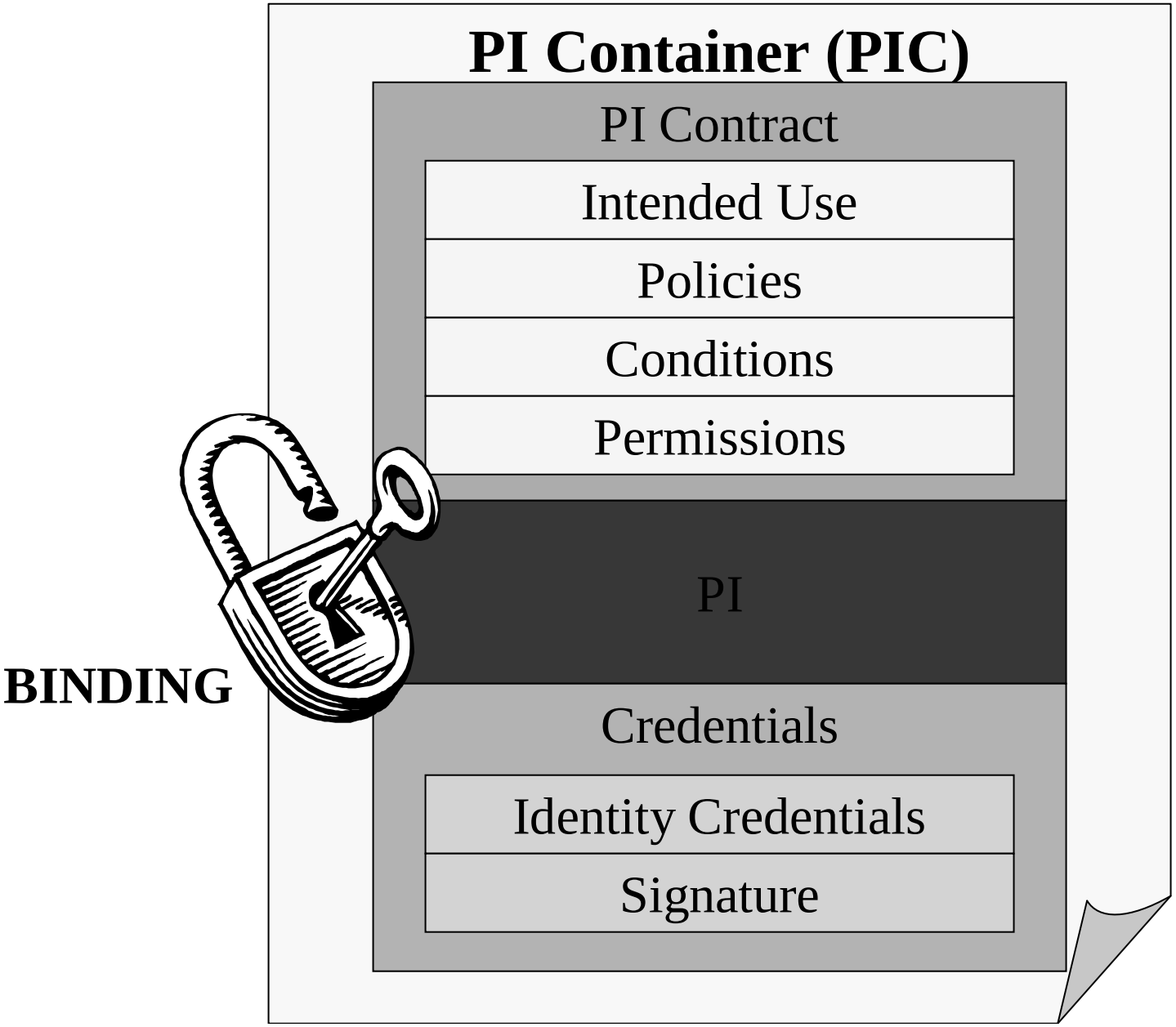
CYCLE

PERMISSION



PERSONAL

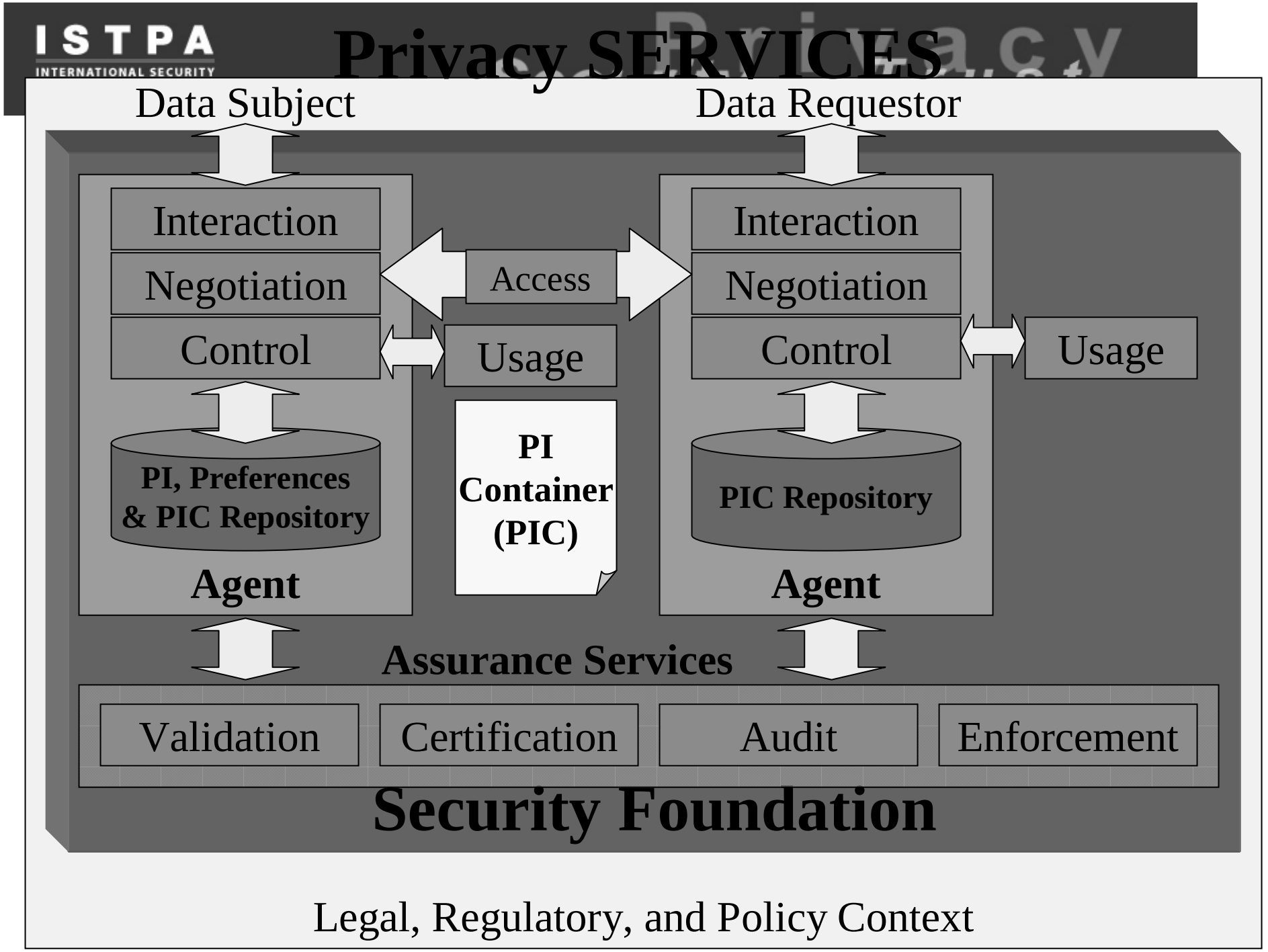
INFORMATION


PI Container (PIC)
PI Contract
Intended Use
Policies
Conditions
Permissions
PI
Credentials
Identity Credentials
Signature
BINDING

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

Access Service: Example Function Set

Access Service provides a means for data subjects to view and modify the PI managed by a data controller or processor. Functions include:

- **Provide a means for the data subject to locate the access mechanism provided by the data controller or processor (if necessary, using the Negotiation Service)**
- **Provide a means to identify and authenticate the data subject or PI owner.**
- **Provide a means to view the data subject's PI, including the agreement(s) negotiated with the data controller or processor.**
- **Modify or delete PI objects, preferences, or agreement as necessary.**
- **Confirm that modifications or deletions have been accepted, executed and recorded by the data controller, processor, certification authority or auditor.**
- **Provide access to the Enforcement Service or its Recourse function, if the data subject believes the terms of a privacy agreement have been violated.**