

Privacy Management Reference Model

**A framework for resolving privacy policy requirements into
operational privacy services and functions**

International Security, Trust & Privacy Alliance

Version 2.0

2009

ISTPA
INTERNATIONAL SECURITY
TRUST & PRIVACY ALLIANCE

Copyright © 1999 – 2009 ISTPA. All rights reserved.

Copyright © 2009 by the International Security, Trust, and Privacy Alliance. All rights reserved.

Published by the International Security, Trust, and Privacy Alliance.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the International Security, Trust and Privacy Alliance.

The International Security, Trust, and Privacy Alliance (ISTPA) has taken care in the preparation of the Privacy Management Reference Model™, but makes no expressed or implied warranty of any kind and assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

For more information, please contact the ISTPA:

Email: info@istpa.org

Website: <http://www.istpa.org>

International Security, Trust, and Privacy Alliance, ISTPA, Privacy Management Reference Model, and Digital Privacy Handbook are all trademarks and/or service marks of the International Security, Trust, and Privacy Alliance. All other company and product names mentioned are used for identification purposes only, and may be trademarks of their respective owners.

ISBN: 978-0-9721484-2-9

Price: \$40.00 U.S.

Table of Contents

1	PREFACE TO VERSION 2.0	4
2	INTRODUCTION	5
2.1	Privacy Management Reference Model Overview	5
2.2	Organization of this Document	6
2.3	About the ISTPA	6
2.4	Acknowledgments	6
3	OPERATIONALLY-FOCUSED PRIVACY REQUIREMENTS	7
4	SECURITY FUNCTIONS AND THE REFERENCE MODEL	10
5	THE TEN PRIVACY SERVICES	11
6	STRUCTURED FORMAT FOR ALL SERVICES	14
7	USING THE PRIVACY MANAGEMENT REFERENCE MODEL	16
8	THE PRIVACY MANAGEMENT REFERENCE MODEL	19
8.1	Core Policy Services	19
8.1.1	Agreement	19
8.1.2	Control	20
8.2	Privacy Assurance Services	21
8.2.1	Validation	21
8.2.2	Certification	22
8.2.3	Audit	24
8.2.4	Enforcement	25
8.3	Presentation and Life Cycle Services	26
8.3.1	Interaction	26
8.3.2	Usage	27
8.3.3	Agent	28
8.3.4	Access	29
9	APPENDIX A: ILLUSTRATIVE USE CASE	30
10	APPENDIX B: ACRONYMS	35

1 Preface to Version 2.0

The original version of the ISTPA Privacy Management Reference Model (formerly called the [Privacy Framework V1.1](#)) was published in May 2002. It was written after extensive consultation with international information protection commissioners and privacy practitioners, as well as much refinement and testing. In it, the ISTPA directly addressed a long-standing problem: privacy requirements (typically expressed as fair information practices or privacy principles) provide little insight into *how* to actually implement them, presenting frustrations for policymakers who expect business systems to manage privacy rules and design challenges for IT architects and solution developers who have few models to guide their work.

The ISTPA Privacy Management Reference Model was developed to aid in the design and implementation of operational privacy management systems. When we vetted the original Reference Model, we confirmed that its 10 privacy Services represented a robust set of operational functions capable of supporting any set of privacy requirements.

However, the state of privacy and information protection has changed substantially since the original ISTPA Privacy Framework was first published in 2002. Today we see accelerated attention to systemic privacy risk and increased expectations of auditable privacy compliance, stemming not only from legislative and regulatory mandates, but also reflecting the business realities of our information-rich IT environment. Today, increased cross-border information flows, networked information processing, use of federated systems, application outsourcing, social networks, ubiquitous devices and cloud computing bring greater challenges and management complexity to privacy risk management.

To address these issues, the ISTPA has completed a series of studies and in-depth exercises aimed at producing an updated revision of the Reference Model. As a starting point and with the understanding that privacy requirements are expressed in different forms (practices, principles, legislation, regulations, and policies), the ISTPA undertook a research project in 2005-2007, analyzing representative global privacy requirements and testing the Reference Model against those requirements.

The results of this analysis were captured in the ISTPA [“Analysis of Privacy Principles: An Operational Study.”](#) published in 2007. Twelve representative international privacy instruments (law, regulations, major statements of privacy principles) were reviewed and core privacy requirements were derived from each instrument. We learned through this process that, while similar words are often used (e.g., notice, consent, etc.), there are significant and subtle differences in their intended meaning and application. Finally, these requirements were grouped together to create a composite set, (shown below in section “Operationally-Focused Privacy Requirements”). The ISTPA has published the complete Analysis of the privacy instruments and other information on its web site: <http://www.istpa.org>.

The findings of this Analysis were then applied to the revision process for the ISTPA Reference Model Services and underlying Functions. As a result of this assessment, we determined that the original Services do provide a robust and comprehensive set of privacy functions to support privacy requirements. Furthermore, this assessment provided a deeper visibility into each Service and its applicability to the nuances of international privacy legislation. This led us to make a number of changes and updates to the Reference Model document.

The ISTPA Privacy Management Reference Model v2.0 is the culmination of this work and has been versioned v2.0 to reflect the fact that the original “framework” has been re-formulated into a “Reference Model” for the implementation of privacy management systems.

Revision Highlights

- The wording of the Service definitions was modified for improved clarity, and extraneous background information was removed.
- We re-formulated the Service/Function definitions into a more systematic format (see section “Structured Format for All Services” for a description). This new format enhances the readability of the Services and is expected to aid in automation and machine implementation of the underlying Functions. The new format is also better suited to modeling and simulation studies.
- Detailed use cases for each Service were removed in order to focus more succinctly on the Service definitions. We recognize that use cases are critical to the effective application of the Reference Model and encourage their development. A sample use case is included in Appendix A.
- The motivational material and background discussion were removed for the same reason. The interested reader is encouraged to read the introductory materials and original use cases in V1.1 on the ISTPA web site.
- The name was changed from Privacy Framework to Privacy Management Reference Model to better reflect the Model’s role in supporting the design of operational implementations for privacy management. Also, we note that the word “Framework” is overused in the literature, particularly as a description of policies, and our use of it for what is essentially a technical model caused confusion and misunderstanding among our readers.
- The foundational role that security plays in privacy was emphasized.
- We changed “data subject” to “individual” in order to be more consistent with current usage.

2 Introduction

2.1 Privacy Management Reference Model Overview

An effective solution to privacy management and compliance obligations in today’s IT-centric, networked systems, services and applications environment would be a collection of policy-configurable, IT-based, systematic behaviors that faithfully satisfy the requirements of privacy policies within a wide variety of contexts and implementation scenarios.

In an operational setting, *privacy is the assured, proper, and consistent collection, processing, sharing, transmission, minimization, use, retention, and disposition of Personal Information (PI) throughout its life cycle, consistent with information protection principles, policy requirements, regulations, and the preferences of the individual.* Since PI has a complex and often extended life cycle, the implication of the definition is that *assured, proper* and *consistent* apply throughout the PI’s life cycle, apply to all actors who have a connection with the information, and apply to all systems and networks to which the information is exposed.

However, any set or combination of fair information practices/principles essentially constitutes a collection of policy objectives or behaviors, and do not by themselves represent a structural Reference Model for defining specific and repeatable functions.

The ISTPA Privacy Management Reference Model provides a solution that enables fair information principles and practices to map to lifecycle privacy functions.

Privacy policy, privacy and security regulations, and associated operational parameters and requirements are treated as inputs within the Reference Model on a contextual basis in support of policy-configurable and adaptable implementations.

This document is intended for anyone responsible for designing and building a privacy management system and, to a lesser degree, for persons responsible for privacy policy who should understand the relationship between privacy requirements (e.g., fair information practices, privacy and security regulations, and derived business policies and processes) on the one hand and the operational functions needed to actually implement those requirements.

The reader is assumed to be familiar with the concepts of privacy, privacy requirements, privacy policy, security, and privacy and security regulations.

2.2 Organization of this Document

A set of working privacy requirements is highlighted, derived from an analysis of representative international privacy instruments and regulations. An Introduction to the ISTPA and the 10 privacy Services composing the ISTPA Privacy Management Reference Model is provided. A structured format for describing the Services is presented in detail, followed by the 10 operational Services, including a definition of each Service and the corresponding Service functions. Appendix A contains an illustrative Use Case involving all 10 Services.

2.3 About the ISTPA

The International Security, Trust, and Privacy Alliance <www.istpa.org> is a global alliance of businesses and technology providers. Our goal is to work together to provide objective and unbiased research and evaluation of privacy standards, tools, and technologies, and to define a Privacy Management Reference Model for building technology solutions.

Within the ISTPA, several working groups were formed, each with a particular area of focus. The Reference Model Working Group is responsible for developing and promoting an objective Reference Model for achieving security, privacy, integrity, and trust in support of global privacy policies and requirements, as described in this document.

The Reference Model Working Group has written the ISTPA Privacy Management Reference Model as a guideline or template for developing operational solutions to privacy issues, as an analytical tool for assessing the completeness of proposed solutions, and as the basis for establishing categories and groupings of privacy management requirements. The Reference Model is not yet a “specification” in the formal sense, but can be used as the basis for a specification or standard.

2.4 Acknowledgments

The ISTPA Privacy Management Reference Model is a joint-volunteer effort made by many ISTPA members who provided insight, commentary and direction.

A special thanks and recognition are due to the Reference Model Working Group and the contributing authors who patiently and diligently created and shaped the content and who collaborated to articulate and design the purpose, benefits and vision of the ISTPA Privacy Management Reference Model.

The Working Group strongly believes that a multi-disciplinary and unifying approach is critical to the successful use of the Privacy Management Reference Model. The problem domain - the complex challenges of security, trust, and privacy - requires extensive collaboration among policymakers and advocates, technical experts, and business owners. If the Privacy Management Reference Model is to be successful, it must remain a collaborative and global effort built with careful attention to the diverse issues and complex technologies that our global information society and digital economy struggle to integrate and resolve.

Reference Model Working Group - AUTHORS

Chair and editor: Michael Willett, Seagate Technology and WillettWorks

John Sabo, CA, Inc.

Adriaan Veldhuisen, Teradata

Kevin O'Neil, CYVA Research

Michele Drgon, DataProbity

ISTPA Board of Directors

The ISTPA Board of Directors volunteers its time to advance the organization's projects and support the several ISTPA Working Groups. ISTPA Board members and officers include:

John Sabo – President, CA, Inc.

Gary Roboff - Vice President, GSR Strategic Consulting

John Lindquist – Treasurer, EWA IIT

Scott Blackmer, Secretary, InfoLawGroup LLP

Michael Willett, Seagate Technology and WillettWorks

Kevin O'Neil, CYVA Research

Michele Drgon, DataProbity

Mike Gurski, Bell Canada

John Hopkinson, EWA/Canada

3 Operationally-Focused Privacy Requirements

In the ISTPA study, **Analysis of Privacy Principles: Making Privacy Operational**, published in 2007, we examined 12 major global privacy instruments and derived a working set of operationally-focused privacy 'requirements' which can be a useful reference for evaluating options for designing and implementing operational privacy controls. These representative operational privacy requirements provide a useful working

set of 'privacy practices' against which to test the applicability of the Privacy Management Reference Model and as a template for more formalized policy statements that can be used in modeling and software engineering applications.

It is important to note that these 'requirements' are operational requirements derived from international instruments having no common definitions, taxonomy or structure. Therefore, these requirements merely represent an attempt to derive commonality, and to make practicable a structured, operational understanding of privacy management and compliance. We recognize that several of the definitions are detailed, but they are intended to reflect as closely as possible operational expectations associated with generic fair information practices/principles.

We are also aware that across international information privacy policy communities, certain terms have existing meanings which may not be acceptable by all stakeholders. For example, the term "individual" may be used in one law or policy instrument and the term "data subject" in another. Other legal instruments use terms such as "consumers" or "the public." For ease of use, this document typically uses the word "individual" to refer to the person whose Personal Information is implicated in the Reference Model services.

In summary, the following requirements are not intended as a substitute for individual policies, laws or regulatory definitions. We believe there would be great value in a standard vocabulary and taxonomy of privacy and policy expressions. In the absence of such standards, the following operational requirements are used in this document for two reasons. First is to demonstrate the utility of the Privacy Management Reference Model as a vehicle to move privacy management, privacy compliance, and privacy control architectures out of the realm of policy debate and into the realm of engineering. Second is to offer an initial set of working definitions that can be used in the "Define" functional category established for each Service (see "Structured Format for All Services").

Accountability: Reporting made by the business process and technical systems which implement privacy policies to the individual or entity accountable for ensuring compliance with those policies, with optional linkages to redress and sanctions.

Notice: Information regarding an entity's privacy policies and practices including: definition of the Personal Information collected; its use (purpose specification); its disclosure to parties within or external to the entity; practices associated with the maintenance and protection of the information; options available to the individual regarding the collector's privacy practices; retention and deletion; changes made to policies or practices; and information provided to the individual at designated times and under designated circumstances.

Consent: The capability, including support for Sensitive Information, Informed Consent, Change of Use Consent, and Consequences of Consent Denial, provided to individuals to allow the collection and/or specific uses of some or all of their Personal Information either through an affirmative process (opt-in) or implied (not choosing to opt-out when this option is provided).

Collection Limitation and Information Minimization: Constraints exercised by the information collector and user to limit the information collected, processed, communicated and stored to the minimum necessary to achieve a stated purpose and, when required, demonstrably collected by fair and lawful means.

Use Limitation: Controls exercised by the information collector or information user to ensure that Personal Information will not be used for purposes other than those specified and accepted by the individual or provided by law, and not maintained longer than necessary for the stated purposes.

Disclosure: The release, transfer, provision of access to, use for new purposes, or divulging in any other manner, Personal Information held by an entity except with notice and consent of the individual; the information collectors policies must be made known to and observed by third parties receiving the information; and sensitive health information disclosures must be managed.

Access and Correction: Capability allowing individuals having adequate proof of identity to find out from an entity, or find out and/or to correct or delete, their Personal Information, at reasonable cost, within reasonable time constraints, and with notice of denial of access and options for challenging denial.

Security/Safeguards: Policies, practices and controls that ensure the confidentiality, availability and integrity of Personal Information collected, used, communicated, maintained, and stored; and ensure that Personal Information will be destroyed or de-identified as required.

Information Quality: Ensures that information collected and used is adequate for purpose, relevant for purpose, not excessive in relation to the purposes for which it is collected and/or further processed, accurate at time of use, and, where necessary, kept up to date, corrected or destroyed.

Enforcement: Mechanisms to ensure compliance with privacy policies, agreements and legal requirements and to give individuals a means of filing complaints of compliance violations and having them addressed, including recourse for violations of law, agreements and policies.

Openness: Availability to individuals of the information collector's or information user's policies and practices relating to their management of Personal Information and for establishing the existence of, nature and purpose of use of Personal Information held about them.

Anonymity: A state in which information is rendered anonymous so that the individual is no longer identifiable.

Information Flow: The communication of personal information across geo-political jurisdictions by private or public entities involved in governmental, economic or social activities.

Sensitivity: Specified information, as defined by law, regulation or policy, which requires specific security controls or special processing.

Illustrative Use Case

Consider the following typical privacy management scenario; mainly, interaction with a service provider that involves exchange of Personal Information.

An individual interacts with a service provider and is considering using certain value-added services, some of which are provided by a third party business partner of the service provider. Selected Personal Information is needed to complete the transaction. The provider indicates what specific PI is needed to initiate the transaction. After checking the privacy policy of the provider, the consumer understands the policy and agrees to provide the PI. The service transaction is initiated. Accuracy of the information provided is checked by the provider and necessary controls needed to secure the PI are also invoked. The provider interacts with the third party business partner to complete the service contract, which involves providing a sub-set of the PI to the third party. This subsequent sharing of PI matches the original purpose of the agreement with the consumer, so third-party sharing is conducted. The provider logs the sharing event. Subsequent misuse of the PI by the third party is detected and corrective action is taken. After receiving notice of the third-party sharing, the consumer requests to see what PI is held by the third party and, if necessary, correct or delete the information.

Illustrative Use Case: Privacy Requirements Identified

Now consider that same Use Case, but this time with the privacy requirements inserted, as defined in the operational set of privacy requirements from the Analysis (listed above).

An individual interacts with a service provider and is considering using certain value-added services, some of which are provided by a third party business partner of the service provider. Selected Personal Information is needed to complete the transaction. The provider indicates what specific PI is needed to initiate the transaction – **COLLECTION LIMITATION AND INFORMATION MINIMIZATION**. After

checking the privacy policy of the provider – **OPENNESS**, the consumer understands the policy and agrees to provide the PI – **CONSENT**. The service transaction is initiated. Accuracy of the information provided is checked by the provider – **INFORMATION QUALITY** – and necessary controls needed to secure the PI – **SECURITY/SAFEGUARDS** – are also invoked. The provider interacts with the third party business partner to complete the service contract, which involves providing a sub-set of the PI to the third party. This subsequent sharing of PI matches the original purpose of the agreement with the individual – **USE LIMITATION**, so third-party sharing – **DISCLOSURE** – is conducted. The provider by agreement has access to event audit logs related to the third party's use of the PI – **ACCOUNTABILITY**. Subsequent misuse of the PI by the third party is detected and corrective action is taken – **ENFORCEMENT**. After receiving notice of the third-party misuse - **ACCOUNTABILITY**, the consumer requests to see what PI is held by the third party and, if necessary, correct or delete the information – **ACCESS and CORRECTION**.

This Use Case demonstrates how the various privacy requirements appear in a typical transaction involving PI. In Appendix A, this Use Case is expanded and the privacy requirements are converted into Reference Model Services.

4 Security Functions and the Reference Model

The original ISTPA Privacy Framework v.1.1 did not directly incorporate security requirements in the privacy services, but did make abundantly clear in both the text and in the accompanying illustrations that information security is an essential component of privacy and that security functions were necessary as a foundation for implementing privacy services. The foundational nature of that relationship cannot be overemphasized.

In undertaking the development of this Reference Model 2.0 revision, ISTPA recognized the importance of more directly establishing an explicit relationship between security requirements and supporting security services (such as confidentiality, integrity and availability services) and the ISTPA Reference Model services (such as Control, Interaction, and Access). Establishing this relationship is critically important in today's environment where, for several years, we have seen an explosion of international information breach headlines raising security issues in the context of privacy. The focus of legislation, media attention, and "headlines" has changed significantly since version 1.1 was released in 2002, and the Reference Model v.2.0 acknowledges more fully the policy and operational relationship among information privacy requirements and security requirements.

ISTPA formally addressed this increased emphasis on security in its 2007 study, *Analysis of Privacy Principles: Making Privacy Operational*. In fact, ISTPA specifically included California State Bill 1386, "Security Breach Notification" among the 12 international laws, directives and model frameworks examined in the *Analysis*. The *Analysis* therefore concluded that security is an explicit component of privacy that would need to be addressed in the new Reference Model.

As noted in the *Analysis*, the EU Data Protection Directive has much to say on this subject, and some of the Member States (notably Austria, Belgium, France, Italy, and Spain, in addition to Norway among the EEA countries) have adopted more detailed regulations on securing Personal Information, especially the more sensitive categories of personal information (typically including health and financial information). Many national and international standards and recommendations exist that are directly relevant to securing personal information in the context of information privacy. Here are just a few representative examples:

- *OECD Information Security Guidelines* [2002]
- *ISO/IEC 27001:2005 - Information technology—Security techniques—Information security management systems—Requirements and ISO/IEC 27002*

- *ISO 15408 Common Criteria*
- The U.S. National Institute of Standards and Technology (NIST) publications such as *FIPS 201, Personal Identity Verification of Federal Employees and Contractors* and *its Computer Security Incident Handling Guide*
- *Payment Card Industry (PCI) Data Security Standard* for securing credit and debit card information and transactions (2005)
- The *ISSEA SSE-CMM (ISO/IEC 21827)*
- *COSO and COBIT* Information Technology control frameworks, used by many companies to assess their information security in connection with Sarbanes-Oxley compliance

Clearly, information security is a robust and well-documented discipline, with multiple international and sectoral standards available to support security policy development, practices, architectures and implementations. The world of information security today certainly has many challenges, both traditional and novel, as organizations adopt new business models and implement new technologies. But as a professional discipline, information security is significantly more advanced than information privacy (with respect to *all* fair information principles and practices, and not simply the “safeguards” or “security” aspects of privacy).

Further proof of this gap between “security” and “privacy” is found in the incredible array of technologies, products and solutions that are available to support information security. Recognizing this rich security environment, ISTPA determined that incorporating detailed security descriptions and functionality lies outside the scope of the Reference Model. Technical standards such as ISO 27001-27002, SAML 2.0, XACML 2.0, X.509, NIST Federal Information Processing Standards (FIPS), the Payment Card Industry Data Security Standard (PCI DSS), and a huge array of other security standards, practices, frameworks and solutions are available to be applied to security risk management requirements for networks, enterprise environments, user systems, applications and software and hardware-based core components of the information and communications infrastructure. Consequently, the Reference Model does not specify any particular security service or mechanism or standard.

Nevertheless, security services are mandatory throughout the lifecycle of PI when required by law, regulation or policy. The privacy services developed in this document must be complemented with appropriate security services and controls (such as strong authentication, information encryption, information loss prevention, access control services, integrity checking, etc.) to satisfy the privacy requirement for security.

The Reference Model 2.0 addresses security in two ways: first, as a foundational layer for the infrastructures which support the collection, storage, communication, sharing and transfer, retention and destruction, processing and lifecycle use of Personal Information, and second, as one of seven specific functions associated with each privacy service. A modular view of the Reference Model (see “The Ten Privacy Services” below) highlights the *foundational* aspect of security. Beyond security as a foundation, each Service incorporates a set of security functions applicable to each Service (see “Structured Format for all Services” below).

5 The Ten Privacy Services

The ISTPA has identified the following list of 10 privacy Services, based on the mandate to support the uniform privacy requirements described above, but at a functional level. A system architect or technical manager should be able to integrate these privacy Services into a functional architecture, with specific mechanisms selected to implement these functions. In fact, the purpose of the ISTPA Privacy Management Reference Model is to stimulate design and analysis of the specific functions - both manual and automatic - that are needed to implement any set of privacy requirements. In that sense, the ISTPA Privacy Management Reference Model is an analytic Reference Model.

To create a usable Reference Model, various system capabilities are identified that typically are not described in privacy practices and principles. For example, a policy management (or control) function is essential to manage the PI usage constraints established by the individual, information collector or regulation, but such a function is not explicitly named in privacy principles/practices. Likewise, interfaces and agents are not explicit in the privacy principles/practices, but are necessary to represent other essential operational services.

Such inferred services are necessary if information systems are to be made “privacy configurable and compliant.” Without them, enforcing privacy requirements in a fully automated environment will not be possible, and government, businesses and individuals will be burdened with inefficient and error-prone manual processing and inadequate privacy governance and compliance controls.

The ISTPA Privacy Management Reference Model defines a “Service” as a collection of related functions and mechanisms that operate for a specified purpose. The ten privacy Services defined in the ISTPA Privacy Management Reference Model are **Agreement, Control, Validation, Certification, Audit, Enforcement, Interaction, Usage, Agent, and Access**. Specific operational behavior of these Services is governed by the privacy policy and parameters configured in a particular implementation and jurisdictional context.

The ISTPA Privacy Management Reference Model encompasses the functions needed to implement uniform privacy requirements, but it is partitioned into subsets of functions that have a logical affinity. The Services listed above can, in total, operationally instantiate and resolve the uniform privacy requirements.

The functions of one Service may invoke the functions of another Service. In other words, one Service may “call” another Service (for example, pass information to the other Service for subsequent action). In this way, the Services can interact in an arbitrary interconnected sequence to accomplish a privacy management task or set of privacy lifecycle requirements. Use cases will illustrate such interactions and their sequencing as the Reference Model is used to solve a particular privacy problem. By examining and by solving multiple use cases, the Reference Model can be tested for applicability and robustness.

The table below summarizes the Services in the ISTPA Privacy Management Reference Model. The table includes a column listing the privacy principles/practices that generally and broadly underlie each Service.

SERVICE	DEFINITION	UNDERLYING PRINCIPLES/PRACTICES
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.	Consent, Collection Limitation, Use Limitation, Disclosure, Access and Correction, Openness, Anonymity, Information Flow, Sensitivity, Notice
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.	Accountability, Use Limitation, Security Safeguards, Information Quality, Notice, Collection Limitation, Access and Correction
VALIDATION	The Validation Service evaluates and, as required, ensures information quality in terms of accuracy, completeness, relevance and timeliness of PI at particular points in the information lifecycle.	Information Quality

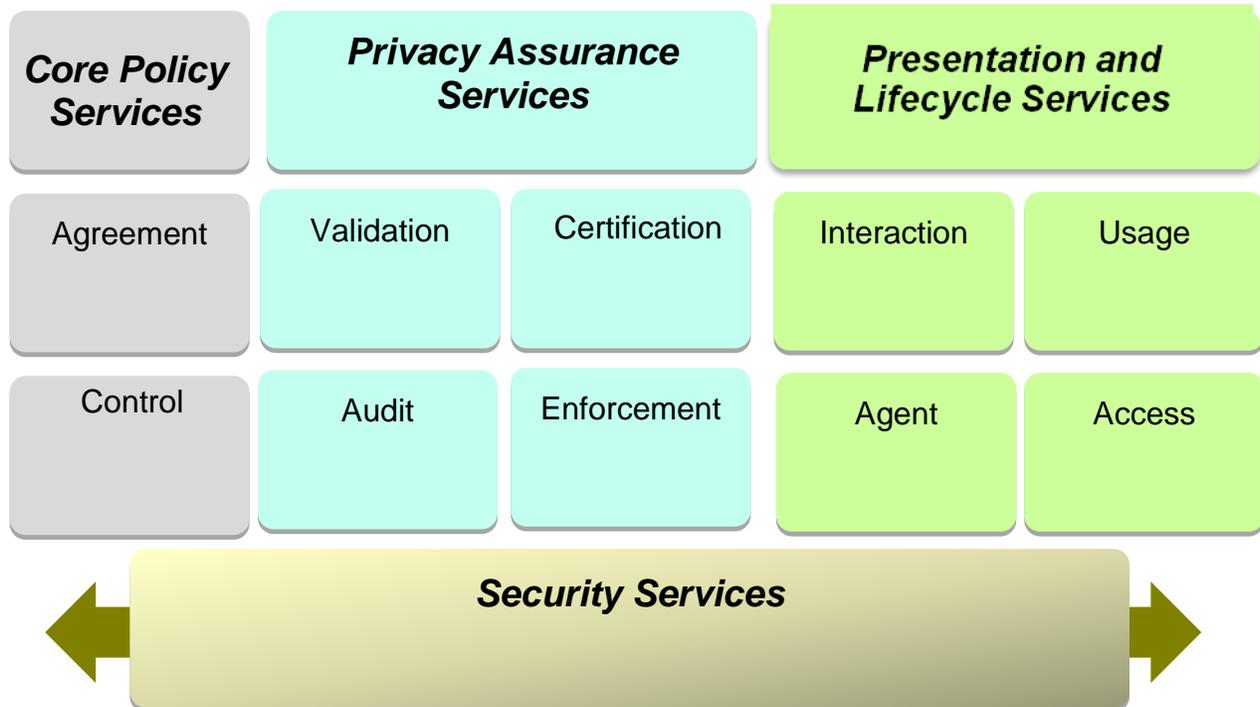
CERTIFICATION	The Certification Service supports the management and validation of credentials of any responsible party or Service involved in processing PI and validates compliance and trustworthiness of an actor or system component with expected policies.	Accountability, Consent, Disclosure, Access and Correction, Security Safeguards, Information Quality, Anonymity
AUDIT	The Audit Service handles the recording and maintenance of service events from other Services. It captures, into privileged audit logs, necessary audit information to ascertain compliance with governing policies and procedures derived from agreements, an organization's internal policies, and any applicable law or regulation.	Accountability, Collection Limitation, Use Limitation, Security Safeguards, Enforcement, Sensitivity
ENFORCEMENT	The Enforcement Service initiates response actions and policy execution when a processing entity does not conform to the terms or policies of an agreement or applicable regulations. Enforcement also includes recourse for individuals when their PI is being used differently from the original agreement.	Accountability, Enforcement, Anonymity, Security Safeguards
INTERACTION	The Interaction Service facilitates a generalized interface as required for presentation, communication, and other movement of relevant information, encompassing functionality not solely associated with privacy, such as user interfaces or system-to-system information exchanges.	Notice, Consent, Collection Limitation, Use Limitation, Disclosure, Access and Correction, Openness, Information Flow, Sensitivity, Security Safeguards, Information Quality, Enforcement
USAGE	The Usage Service ensures that the active use of PI, when outside the control of the individual, complies with the terms and policies of any agreement and applicable regulation at any point in the lifecycle of PI. The Usage Service monitors processes and functions, such as information minimization, linking, integration, inference, transfer, derivation, aggregation, and pseudo-anonymization of PI.	Use Limitation, Openness, Anonymity, Information Flow, Sensitivity, Accountability, Notice, Access and Correction, Information Quality
AGENT	The Agent Service is a process that acts on behalf of an individual or processing entity at any point in the lifecycle of PI.	Accountability, Notice, Consent, Collection Limitation, Use Limitation, Disclosure, Access and Correction, Security Safeguards, Openness, Anonymity, Information Flow, Sensitivity
ACCESS	The Access Service enables, as required by policy or regulation, individuals to review their PI at any point in the lifecycle and, if required by policy, have the ability to submit changes to their PI.	Consent, Disclosure, Access and Correction, Security Safeguards, Information Flow, Openness

The 10 Services can be logically grouped into several categories:

- **Core Policy:** Agreement, Control
- **Privacy Assurance:** Validation, Certification, Audit, Enforcement
- **Presentation and Lifecycle:** Interaction, Agent, Usage, Access

These groupings, illustrated below, are meant to clarify the “architectural” relationship of the Services in an operational design. However, all Services are available for mutual interaction without restriction.

Privacy Reference Model



NOTE: The reader who is not interested (at least, initially) in reviewing the detailed Service functional definitions can skip to Section “[APPENDIX A: Illustrative Use Case](#)”.

6 Structured Format for all Services

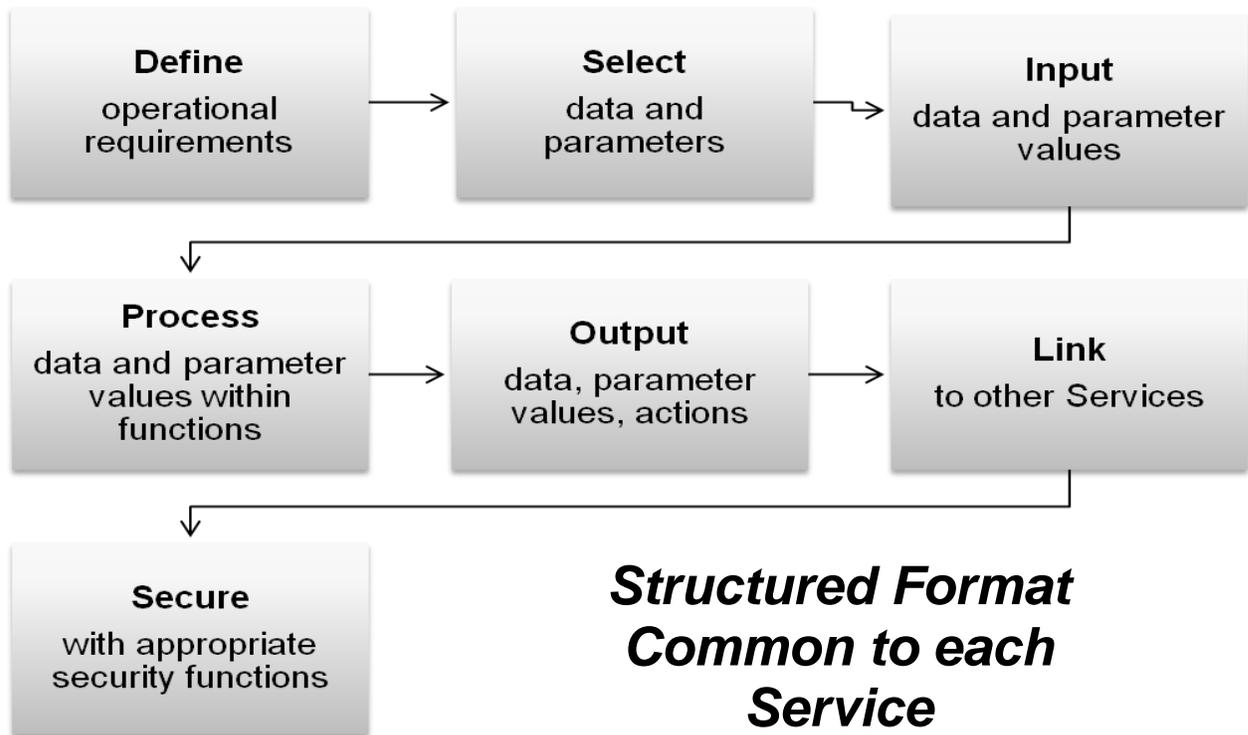
For the purpose of describing the functional characteristics of the 10 Services, the ISTPA has developed a structured format for each Service (SVC). Besides providing a uniform description, the format will facilitate automated implementation and analytic modeling of the Services.

Functions Associated with all Services

Each Service is composed of functions from seven functional categories that comprise the syntax for the ten Services:

1. **DEFINE [SVC]** operational requirements
2. **SELECT [SVC]** (input, process, and output) information and parameters
3. **INPUT [SVC]** information and parameter values in accordance with Select
4. **PROCESS [SVC]** information and parameter values within Functions
5. **OUTPUT [SVC]** information, parameter values, and actions
6. **LINK [SVC]** to other (named) Services

7. **SECURE [SVC]** with the appropriate security functions



Some functions may be used multiple times in both defining and executing the Service, and so the illustration above is greatly simplified. For example, if multiple functions are defined for a particular Service, then the function 'Process' is referenced multiple times in the definition of that Service and in the invocation of that Service in particular Use Cases.

In fact, different Use Cases will engage distinct requirements, will require specific input/output parameters, will invoke a varied subset of the Service Functions, and will link specific Services. That is, each Use Case leads to a customized combination and sequence of the seven functions above. By using a structured format, each Use Case will have the same structural appearance, lending itself to ease of automation and modeling.

A more detailed description of the seven functions used to implement each Service follows:

DEFINE operational requirements - documentation of specific *operational* requirements driving the use of a particular Service and its functionality.

- Privacy and privacy-related requirements come in many forms, including as principles, practices, and legal or regulatory requirements. These requirements can be described as policy-level requirements.

- Cull through these formal and informal requirements for the pertinent list of requirements. Such “raw” policy requirements need to be transformed into *operational* requirements in order to apply the Reference Model Services.

SELECT input, process and output information and parameters mandated by the requirements.

- As part of identifying the operational functions needed, the functional parameters for input, process, and output need to be identified to assist in setting the scope of the Service.

INPUT information and parameter values in accordance with Select

- Populate the Service with both information associated with the requirements and with functional parameters necessary for Service execution. Before each appropriate Service function is executed, the specific parameters necessary to the operation of that function need to be identified as source for the Service processing.

PROCESS information and parameter values - execution of the Service, operating on the input parameters

- Each Service Function is executed, operating on the parameters that were previously selected as Input, and to prepare for the selected Output.
- A given Service may have many such specific functions that could be executed in a given context or Use Case.

OUTPUT information, parameter values and actions - operational results produced as a product of the Service processing.

- After each Service Function is executed, relevant operational results are produced as a product of the Service processing.

LINK communications with one or more of the other Services and their Functions

- In any privacy management Use Case scenerio, the various Services are interconnected, with specific Services immediately connected to other Service(s) from an Input and Output perspective.
- Which Services are “linked” depends on the specific context or Use Case under study. Conceivably, any Service can be linked to any other Service.

SECURE with the appropriate security functions

- Security is an essential element to each Service, providing policy, process, and technical controls necessary to ensure that confidentiality, integrity, and availability are enforced for the accurate and trustworthy processing of Personal Information and the execution of all Services.
- As applied to specific Services, the appropriate security functions, such as information encryption, non-repudiation, authentication, and authorization, must be based on a risk analysis appropriate for a particular use case and risk management environment.

7 Using the Privacy Management Reference Model

The first step in applying the operational Services is to establish an initial set of operational, privacy policy-driven requirements, because that is the basis for moving to the next step in determining which Reference Model Services and their underlying Functions need to be invoked. This is a critical and creative step,

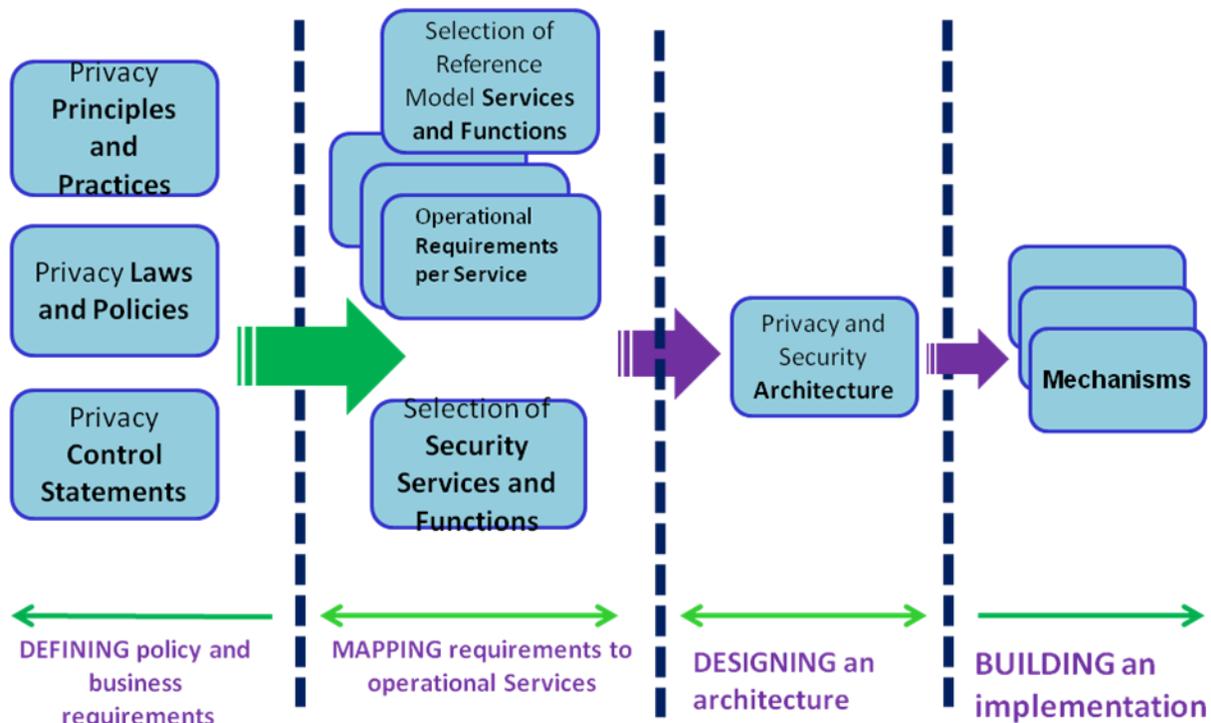
because the business 'requirements' related to privacy do not always first appear in clear or concise form. (The ISTPA *Analysis of Privacy Principles: An Operational Study* illustrates a methodology for deriving clear policy-level requirements from multiple, dissimilar policy instruments such as laws and directives.)

Policy-level requirements can then be transformed into a set of operational requirements usable by IT architects and business process managers. The Analysis document offers a working set of policy-level requirements that was used to test the Reference Model Services.

The first Service function is "Define [SVC] operational requirements", as part of the pre-configuration for a specific context or Use Case. The privacy management implementer must transform policy-level requirements into the operational requirements expected by the function **Define**. For example, at the policy requirement level, the privacy principle, *Use Limitation*, may be defined from an operational perspective generally as "controls exercised by the information collector or information user to ensure that Personal Information will not be used for purposes other than those specified and accepted by the individual or provided by law, and not maintained longer than necessary for the stated purposes." Such an operational, general descriptor may then be used to drive more detailed business process and technical modeling, which in turn can be used to identify requirements usable by specific Reference Model Services.

Therefore, only after policy-level requirements have been clearly identified and expressed, their implementation requires additional analysis to express specific operational requirements, which in turn leads to determining which Reference Model Services are required, what functionality available for each service is to be used, how the Services will interact over the lifecycle of the information, and what specific parameters must be included which affect the functionality (e.g., time-dependencies or unique requirements for highly sensitive information).

Illustrations of this process are best done through use case development. However, the iterative illustration below is informative.



Policy and business requirements related to privacy are mapped into Reference Model Services and Functions by first identifying the operational requirements for each Service. Necessary security functions are also selected. The results of this operational, mapping phase are then designed into an appropriate architecture. Finally, the architecture provides the ‘blueprint’ for selecting the corresponding Mechanisms for building an actual implementation.

The Privacy Management Reference Model is intended to be a baseline for further development, including the possibility of adoption and refinement by recognized standards organizations. However, in its current form it can prove valuable to stakeholders – whether business program managers, technically-oriented policymakers, or technical managers and implementers - who understand their obligations to manage privacy policies and obligations in today’s networked and distributed computing environments, but who do not have a usable structure in which to frame their architectural designs and implementation requirements.

The Reference Model’s concepts of **Core Policy Services**, **Privacy Assurance Services**, **Presentation and Lifecycle Services**, and underlying **Security Services** and their associated functions support the development of structured use cases applicable to business functions governed by privacy requirements, such as management of electronic health records or Personal Information transferred cross-border and subject to cross-jurisdictional rules. Modeling tools can be applied to the Reference Model to improve automated and policy-directed privacy management systems. For example, professional Requirements Management Tools can facilitate future engineering efforts and provide greater accessibility and use by stakeholders.

The Reference Model intentionally does not identify mechanisms or tools that are currently available to support its services and functions (mechanisms such as technical security protocols; information loss prevention technologies; identity, authentication and authorization technologies; Extensible Markup Language messaging standards; policy rules engines; and others). The mapping of both currently available and new mechanisms to Reference Model services and functions is out of scope of this document, but is a necessary next step in delivering operational, trans-jurisdictional, auditable and trusted lifecycle privacy management systems.

8 The Privacy Management Reference Model

In the next ten major sections, the structured format is used to define the 10 operational Services in a formal way. For purposes of exposition, the Services are listed alphabetically. Each section has the same structure:

- Definition
- Functions

8.1 Core Policy Services

8.1.1 Agreement

Agreement Definition [AGR_DEF]

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.

Agreement Functions [AGR_FNC]

DEFINE Agreement requirements AGR-D1

- o Establish objectives and scope for the Agreement service
- o Document/obtain Agreement rules and standards
- o Document the applicable interfaces that exist or are required

SELECT Agreement parameters or Input, Process, and Output AGR-S1

- o Identify the different parties and classes of Agreement
- o Identify Agreement transactions that need to be recorded

INPUT Agreement of PI definition AGR-I1

- o Construct an agreement that defines what PI is requested, to what purpose(s), and whether it is required or optional so that the processing entity is making an informed decision

INPUT Agreement for additional permissions AGR-I2

- o Construct an agreement that defines additional permissions requested, for what purpose(s), for which PI, and whether these permissions are required or optional

PROCESS Agreement parameters AGR-P1

- o Construct parameters governing information collection and use for presentation to the individual (e.g., what PI is collected, what purpose it will be used, policies and options) or entity

PROCESS Agreement exchange **AGR-P2**

- Exchange initial parameters related to a potential agreement between parties

PROCESS Agreement interchange **AGR-P3**

- Interchange conditional agreements between parties

OUTPUT Agreement results **AGR-O1**

- Output the consent, denial or an agreement among the parties

LINK Agreement to another Service **AGR-L1**

- Connect Agreement with another Service and pass outputs and other parameters between Agreement and that Service, as appropriate

SECURE Agreement **AGR-SEC1**

- Invoke security controls in support of Agreement functions, as appropriate

8.1.2 Control

Control Definition [CTL_DEF]

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.

Control Functions [CTL_FNC]

DEFINE Control requirements **CTL-D1**

- Establish objectives and scope for the Control service
- Document/obtain control rules and standards

SELECT Control parameters For Input, Process, and Output **CTL-S1**

- Identify linkage to services (or functions) to control
- Develop a process for each control function, or identify/obtain control mechanisms that could be applied
- Make control functions available to Services

INPUT Control association to PI usage **CTL-I1**

- Associate PI to a information usage agreement

INPUT Control rules from Policy **CTL-I2**

- Receive specifically defined rules and policy from the processing entities.

(Note: Operation of the Control Service is governed by laws, regulations, policies, and information usage agreements)

PROCESS Control configuration **CTL-P1**

- Configure the Control function in accordance with prescribed privacy policies and controls

PROCESS Control management **CTL-P2**

- Manage PI in accordance with prescribed privacy policies and controls

PROCESS Control of PI input/output **CTL-P3**

- Allow PI to flow in and out of the repositories, subject to prescribed policies and controls

OUTPUT Control interaction with internal parties or systems **CTL-O1**

- Interact directly with internal parties

(Note: Internal parties or systems are defined as those requestors that are either indirectly or explicitly bound to the terms of information usage and privacy agreements)

OUTPUT Control interaction with external parties or systems **CTL-O2**

- Interact indirectly with external parties

(Note: External parties or systems are entities that are seeking PI from the PI processing entity. External parties are not implicitly bound by information usage or privacy agreements, nor are they considered part of the information processing entity)

LINK Control to another Service **CTL-L1**

- Connect Control with another Service and pass outputs and other parameters between Control and that Service, as appropriate

SECURE Control **CTL-SEC1**

- Invoke security controls in support of Control functions, as appropriate

8.2 Privacy Assurance Services

8.2.1 Validation

Validation Definition [VAL_DEF]

The Validation Service evaluates and, as required, ensures information quality in terms of accuracy, completeness, relevance and timeliness of PI at particular points in the information lifecycle.

Validation Functions [VAL_FNC]

DEFINE Validation requirements **VAL-D1**

- Check for consistency requirements against defined bounds and heuristics

- Establish objectives and scope for the Validation service
- Document/obtain validation rules and standards
- Maintain requirements/tools to record (in)validation

SELECT Validation parameters for Input, Process, and Output

VAL-S1

- Determine information objects that need to be validated
- Identify the different object classes and their means of validation
- Document the applicable mechanisms and tests that exist
- Identify validation tools that need to be created/added

INPUT Validation for comparison of information

VAL-I1

- Compare information objects based on requirements being entered to both information that the individual has previously entered, and to related and supporting elements

PROCESS Validation for accuracy

VAL-P1

- Evaluate PI for accuracy

PROCESS Validation for completeness

VAL-P2

- Evaluate PI for completeness

PROCESS Validation for relevance

VAL-P3

- Evaluate PI for relevance

PROCESS Validation for timeliness

VAL-P4

- Evaluate PI for timeliness

OUTPUT Validation of validity check

VAL-O1

- Alert the system as to results of validity check

LINK Validation to another Service

VAL-L1

- Connect Validation with another Service and pass outputs and other parameters between Validation and that Service, as appropriate

SECURE Validation

VAL-SEC1

- Invoke security controls in support of Validation functions, as appropriate

8.2.2 Certification

Certification Definition

[CRT_DEF]

The Certification Service supports the management and validation of credentials of any responsible party or Service involved in processing PI and validates compliance and trustworthiness of an actor or system component with expected policies.

Certification Functions [CRT_FNC]

DEFINE Certification requirements CRT-D1

- Ascertain relevant privacy policies and/or regulatory requirements, and assemble necessary criteria for certification
- Identify the different parties to certification
- Establish objectives and scope for the Certification service
- Document/obtain certification rules and standards

SELECT Certification parameters for Input, Process, and Output CRT-S1

- Select certification tools and compliance mechanisms

INPUT Certification workflow progress CRT-I1

- Deploy interaction with existing privacy and security processes
- Execute a continuous method of compliance demonstration
- Maintain audit and validation of workflow progress for PI processing entities under review by the Certification process

PROCESS Certification of credential management CRT-P1

- Manage the credentials of any responsible party or Service

PROCESS Certification of credential affirmation CRT-P2

- Validate the credentials of any responsible party or Service

PROCESS Certification of Compliance CRT-P3

- Check the compliance and trustworthiness of actor/system with policies and requirements

OUTPUT Certification status of Process functions CRT-O1

- Report the success or failure to validate credentials of any responsible party or compliance status of an actor or system component with expected policies

OUTPUT Certification compilation of histories CRT-O2

- Compile certification credential issuance and revocation histories for examination

LINK Certification to another Service CRT-L1

- Connect Certification with another Service and pass outputs and other parameters between Certification and that Service, as appropriate

SECURE Certification CRT-SEC1

- Invoke security controls in support of Certification functions, as appropriate

8.2.3 Audit

Audit Definition

[AUD_DEF]

The Audit Service handles the recording and maintenance of service events from other Services. It captures, into privileged audit logs, necessary audit information to ascertain compliance with governing policies and procedures derived from agreements, an organization's internal policies, and any applicable law or regulation.

Audit Functions

[AUD_FNC]

DEFINE Audit requirements

AUD-D1

- Establish objectives and scope for the Audit service
- Document/obtain audit rules and standards

SELECT Audit parameters for Input, Process, and Output

AUD-S1

- Set up secure audit logs and authentication/authorization
- Identify all transactions to be recorded
- Develop the audit process

INPUT Audit parameters

AUD-I1

- Input includes log of PI, agreement and preference, including authoring, access, modification and erasure permissions

PROCESS Audit recording

AUD-P1

- Record events from other Services

PROCESS Audit maintenance

AUD-P2

- Manage changes to the Audit process

PROCESS Audit of audit log association

AUD-P3

- Persistently associate an audit log with events throughout the life cycle of PI

PROCESS Audit policy compliance

AUD-P4

- Check compliance against governing policies and procedures derived from agreements, an organization's internal policies, and any applicable law or regulation

OUTPUT Audit consolidated reports on PI

AUD-O1

- Maintain audit reports
- Transform the association of audit log(s) across several instantiations or versions of PI objects, and provide consolidated reports of PI processing across processing entities

OUTPUT Audit non-compliance reports and alerts

AUD-O2

- Issue reports and alerts for non-compliance with governing policies and procedures derived from agreements, an organization's internal policies, and any applicable law or regulation

LINK Audit to another Service **AUD-L1**

- Connect Audit with another Service and pass outputs and other parameters between Audit and that Service, as appropriate

SECURE Audit **AUD-SEC1**

- Invoke security controls in support of Audit functions, as appropriate

8.2.4 Enforcement

Enforcement Definition [ENF_DEF]

The Enforcement Service initiates response actions and policy execution when a processing entity does not conform to the terms or policies of an agreement or applicable regulations. Enforcement also includes recourse for individuals when their PI is being used differently from the original agreement.

Enforcement Functions [ENF_FNC]

DEFINE Enforcement requirements **ENF-D1**

- Establish objectives and scope for the Enforcement service
- Document/obtain enforcement rules and standards

SELECT Enforcement parameters for Input, Process, and Output **ENF-S1**

- Obtain access rules and the agreed policies terms to enforce
- If required, develop and agree on consequences or recourse
- Develop a distinct enforcement process for each rule
- Identify/obtain mechanisms necessary to support rules

INPUT Enforcement access to complaints **ENF-I1**

- Provide individuals, processing entities, regulatory authorities and enforcement entities access to complaint/remedy methods, as appropriate

INPUT Enforcement remedy to complaints **ENF-I2**

- Provide regulatory authorities and enforcement entities, both internal and external, the means to impose remedies, or corrective actions, and to secure relief on behalf of individuals and information processing entities

PROCESS Enforcement of response actions and policy execution **ENF-P1**

- Initiate response actions and policy execution when a processing entity does not conform to the terms or policies of an agreement or the applicable regulations

PROCESS Enforcement invocation of recourse actions **ENF-P2**

- Execute identified recourse and remediation actions for policy violations

OUTPUT Enforcement of findings

ENF-O1

- Provide the means for individuals, processing entities, certification authorities, regulatory authorities, enforcement agencies, and judicial authorities as appropriate to examine investigative findings

LINK Enforcement to another Service

ENF-L1

- Connect Enforcement with another Service and pass outputs and other parameters between Enforcement and that Service, as appropriate

SECURE Enforcement

ENF-SEC1

- Invoke security controls in support of Enforcement functions, as appropriate

8.3 Presentation and Life Cycle Services

8.3.1 Interaction

Interaction Definition

[INT_DEF]

The Interaction Service facilitates a generalized interface as required for presentation, communication, and other movement of relevant information, encompassing functionality not solely associated with privacy, such as user interfaces or system-to-system information exchanges.

Interaction Functions

[INT_FNC]

DEFINE Interaction requirements

INT-D1

- Identify the different classes of interaction, related to privacy policies
- Establish objectives and scope for the Interaction service
- Document/obtain interaction rules and standards

SELECT Interaction parameters for Input, Process, and Output

INT-S1

- Identify classes of interaction for sensitive information
- Document the applicable interfaces that exist
- Develop interaction that needs to be created/added
- Develop interaction controls for these new/additional interfaces

INPUT Interaction presentation information

INT-I1

- Compose the presentation of information between internal and external entities, such as input of the individual's PI, the individual's privacy preferences, and actions, as well as confirmation of actions

INPUT Interaction from Agent **INT-I2**

- Compose the external interface to the Agent in cases where an Agent is used
- (Note:** The Interaction Service provides a generalized interface and presentation function)

PROCESS Interaction presentation **INT-P1**

- Present relevant information

PROCESS Interaction communication **INT-P2**

- Communicate, move, or exchange relevant information

OUTPUT Interaction to Agent **INT-O1**

- Provide the external interface to the Agent in cases where an Agent is used.
- (Note:** The Interaction Service provides a generalized interface and presentation function)

OUTPUT Interaction of information representation
INT-O2

- Includes mechanisms and methods for information representation, multi-modal I/O (on and off line), communications interfaces, storage of raw information, traditional presentation services (e.g., GUIs), as well as external machine and automation interfaces

LINK Interaction to another Service **INT-L1**

- Connect Interaction with another Service and pass outputs and other parameters between Interaction and that Service, as appropriate

SECURE Interaction **INT-SEC1**

- Invoke security controls in support of Interaction functions, as appropriate

8.3.2 Usage

Usage Definition [USG_DEF]

The Usage Service ensures that the active use of PI, when outside the control of the individual, complies with the terms and policies of any agreement and applicable regulation at any point in the lifecycle of PI. The Usage Service monitors processes and functions, such as information minimization, linking, integration, inference, transfer, derivation, aggregation, and pseudo-anonymization of PI.

Usage Functions [USG_FNC]

DEFINE Usage requirements **USG-D1**

- Establish objectives and scope for the Usage service
- Document/obtain usage rules, standards and capabilities

SELECT Usage parameters for Input, Process, and Output **USG-S1**

- identify information usage types that needs to be monitored
- document the different means of monitoring information usage
- identify the applicable processes that exist
- develop the usage processes that need to be added

INPUT Usage Rules for PI **USG-I1**

- Identify and transfer to the processing entity the terms and policies of any agreement and applicable regulation governing the use of PI

PROCESS Usage compliance **USG-P1**

- Ensure that the active use of PI complies with the terms and policies of any agreement and applicable regulation at any point in the lifecycle of that PI

PROCESS Usage of evolving PI **USG-P2**

- Monitor processes and functions, such as information minimization, linking, integration, inference, transfer, derivation, aggregation, and anonymization of PI

OUTPUT Usage Processing reports **USG-O1**

- Output reports derived from the processing, use, communication or destruction of PI

OUTPUT Usage conditions impacting agreements **USG-O2**

- Output conditions associated with the processing of PI

LINK Usage to another Service **USG-L1**

- Connect Usage with another Service and pass outputs and other parameters between Usage and that Service, as appropriate

SECURE Usage **USG-SEC1**

- Invoke security controls in support of Usage functions, as appropriate

8.3.3 Agent

Agent Definition [AGT_DEF]

The Agent Service is a process that acts on behalf of an individual or processing entity at any point in the lifecycle of PI.

Agent Functions [AGT_FNC]

DEFINE Agent requirements **AGT-D1**

- Establish objectives and scope for the Agent service
- Document/obtain agent rules and standards; identify recording mechanisms for agent agreements

SELECT Agent parameters for Input, Process, and Output **AGT-S1**

- Identify the different agent mechanisms representing individuals and entities

INPUT Agent interfaces **AGT-I1**

- Document the applicable agent interfaces/processes that exist
- Identify agent interfaces/processes that need to be created
- Provide storage of information about PI objects, agents, preferences, and agreements

INPUT Agent specification **AGT-I2**

- Provide a means for an actor or entity to specify an agent to enter PI objects, preferences and agreements governing PI object access and processing

PROCESS Agent invocation **AGT-P1**

- Invoke Services on behalf of an individual or processing entity

OUTPUT Agent Service invocation results **AGT-O1**

- Output the results of the Agent invocation of a Service

LINK Agent to another Service **AGT-L1**

- Connect Agent with another Service and pass outputs and other parameters between Agent and that Service, as appropriate

SECURE Agent **AGT-SEC1**

- Invoke security controls in support of Agent functions, as appropriate

8.3.4 Access

Access Definition [ACC_DEF]

The Access Service enables, as required by policy or regulation, individuals to review their PI at any point in the lifecycle and, if required by policy, have the ability to submit changes to their PI.

Access Functions [ACC_FNC]

DEFINE Access requirements **ACC-D1**

- Establish objectives and scope for the Access service;
- Document/obtain access rules and standards

SELECT Access parameters for Input, Process and Output **ACC-S1**

- Identify the different classes of information access and the means of access
- INPUT Access external views to PI and agreements** **ACC-I1**
- Document the external interfaces that exist for individuals
 - Provide the external means to view the individual's PI, including the agreement(s) negotiated with the processing entity or entities
- INPUT Access internal views to PI** **ACC-I2**
- Document internal interfaces for processing entities
 - Identify access that needs to be created/added/revoked
 - Provide a means for the individual to locate the access mechanism provided by the information controller or processor (if necessary, using the Agreement Service)
- PROCESS Access review** **ACC-P1**
- Enable, as required by policy or regulation, individuals to review their PI
- PROCESS Access change submission** **ACC-P2**
- Enable, as required by policy or regulation, individuals to submit changes to their PI
- OUTPUT Access change result** **ACC-O1**
- Provide confirmation of result of change request
- LINK Access to another Service** **ACC-L1**
- Connect Access with another Service and pass outputs and other parameters between Access and that Service, as appropriate
- SECURE Access** **ACC-SEC1**
- Invoke security controls in support of Access functions, as appropriate

9 APPENDIX A: Illustrative Use Case

In order to illustrate how the Privacy Management Reference Model can be applied, we have developed an abstract, generic use case in which a representative set of privacy requirements is “converted” or mapped to necessary Reference Model Services. In this example, specific “context” and jurisdictional details have been suppressed in order to focus on the conversion process. Routine calls (for example) to Interaction for information exchange and inquiry are not shown, in order to clearly highlight the relationship between requirements and Services. This Use Case is based on the typical privacy management scenario introduced earlier.

In this scenario:

- (1) an organization identifies the laws, rules and policies associated with its use of PI for an application
- (2) the information requestor seeks Personal Information from an individual

- (3) an agreement is reached between the individual and the requestor
- (3) the information and permissions are provided
- (4) the information requestor uses the PI
- (5) the information requestor shares PI and permissions with a third party
- (6) the third party attempts to use the PI
- (6) An inappropriate use is blocked and an enforcement process initiated
- (6) The individual requests access to check on information maintained by the third party

Conversion Steps (mapped to numbers above):

1: Identify the privacy principles/practices and policy rules that must be applied to PI requested, collected, and used for this application.

These parameters are used to configure the Control Service and other Services. For example:

- Specific PI information elements to be collected
- Rules governing usage by Requestor
- Rules governing transfer to Third Party
- Policies governing individual access, enforcement and redress

Control	Initialization/configuration of Policy/Rules
----------------	---

2: A PI Requestor solicits PI from an Individual.

In this conversion step, the information requestor establishes a channel for interacting with the individual, using the Interaction Service. In this instance, an Agent is used as a vehicle to communicate with the individual. This interchange reflects policies already established in Step 1. Credentials are checked to ensure the agent actually represents the information requestor, and the information requests and responses are transacted, including both information and policy elements such as PI elements, conditions for use of PI, enforcement promises, etc.

Interaction	Defined/initialized
Agent	Individual and Requestor use software Agents
Interaction	Requestor contacts Individual using Agents
Interaction	Requestor provides credentials to Individual
Certification	Individual checks and accepts validity of

	credentials
Agreement	Requestor makes initial request for PI, provides desired conditions and purpose

3: The Individual and Requestor reach an agreement as to what PI will be provided and with what permissions; and, PI is transferred to the Requestor.

In the third step, the Interaction service continues to serve as an interface to deliver necessary information to both parties related to the request for information, handled by the Agreement Service via the Agent Service. The Individual selects a set of options presented by the Requestor, and these are communicated via the Agent Service back to the Requestor. The Requestor creates an agreement language, which in this example is slightly modified from the initial request. Individual confirms approval of the agreement, The Audit Service records that this negotiated agreement occurred and the Control Service linked to the Agreement is updated for both the Individual and Requestor to reflect the specific terms and conditions. A linkage is made to the Usage Service to establish permissible and impermissible actions. PI is transferred to the Requestor and the Audit Service records the transfer. Finally, the Validation Service checks information quality.

Agent	Agents continue to represent Individual and Requestor
Agreement	Individual selects desired permission modification
Agreement	Requestor (and Individual) agree
Audit	Negotiated agreement recorded
Interaction	PI + permissions transferred to Requestor
Audit	Records transfer
Control	Stores PI and agreement
Validation	Checks PI information quality

4: The Requestor subsequently uses the PI.

Usage (+ Control) governs the subsequent use of the PI by the Requestor, subject to the agreed-to permissions and rules. Audit records any use by the Requestor.

Usage	Usage links to Control to access usage policies governing subsequent use of PI
Usage	Usage monitors attempted uses of PI by Requestor application
Audit	Records use of PI

5: The Requestor transfers the PI + permissions to a third party.

Through Agreement, the third party makes an initial request for the Individual's PI using the Interaction Service, including proposed uses, associated policies and other information relevant to the request. Requestor and Third Party exchange credentials using the Certification Service. Requestor accepts Third Party credentials, associates the contents of the request with policies contained in the Control Service, and confirms that the purpose and conditions are consistent with the agreement made with the Individual governing any subsequent transfer. Through Agreement, Requestor agrees to the transfer to the third party and an agreement is confirmed. Audit records that this negotiated transaction occurred. PI with allowed permissions is transferred to the third party. Audit records the transfer. Control (for both Requestor and third party) records/stores/links the transaction, including the PI + permissions, in a repository. Validation checks the information quality of the PI provided.

Interaction	Establishes communication between the Requestor and Third Party
Agreement	Third party makes initial request for PI, provides desired conditions and purpose
Certification	Checks to ensure Third Party is authorized to receive PI
Control	Linkage to Control establishes rules governing PI transfers to Third Party
Agreement	Requestor agrees to transfer PI
Audit	Audit records agreement
Interaction	PI + permissions transferred to third party
Audit	Audit records transfer of PI
Control	Stores PI + agreement
Validation	Checks PI information quality

6: The third party attempts an improper use of the PI.

Monitored by Usage, the third party attempts to use the PI in a way not permitted by the Individual. Usage raises an Alert that is recorded by Audit. Enforcement is invoked and the designated recourse is taken. Having learned that the third party holds Individual PI, the Individual requests Access to the PI held by the third party.

Interaction	Third Party Application makes call to PI
Interaction	Interaction links application to Usage Service
Usage	Usage monitors Third Party use of PI and determines it is not permitted by agreement policy

Usage	Usage issues alert and links to Audit and Enforcement Services
Enforcement	Initiates Recourse action and notifies Individual
Access	Individual is notified of invalid use attempt and requests Access to PI maintained by Third Party

The next step in the conversion would be to identify the specific functions (drawn from the seven canonical functions under each Service) invoked for each Service that is engaged in the use case (*not done here*).

Security:

Note that at each step in the process above, relevant security functions should be invoked in accordance with security risk assessments. For example:

- The interaction among the parties may require identity, authentication and authorization controls and information encryption.
- Certification may make use of both authentication and authorization controls to check the identity of the parties as well as ensure policy rule integrity.
- The Control database may employ integrity, availability and access control techniques.
- Integrity measures may be invoked for any transferred information.
- Secure time stamping may be associated with relevant events.

10 APPENDIX B: Acronyms

COBIT: Control Objectives for Information and Related Technology

COSO: Committee of Sponsoring Organizations

EU: European Union

FIPS: Federal Information Processing Standard

FISMA: Federal Information Security Management Act

IEC: International Electro-technical Commission

ISO: International Standards Organization

ISSEA: International Systems Security Engineering Association

ISTPA: International Security, Trust and Privacy Alliance

NIST: National Institute of Standards and Technology

OECD: Organization for Economic Cooperation and Development

PCI DSS: Payment Card Industry Data Security Standard

PI: Personal Information

SAML: Security Assertion Markup Language

SSE-CMM: Systems Security Engineering – Capability Maturity Model

XACML: eXtensible Access Control Markup Language