COPY OF CHARTER FOR OASIS Privacy Management Reference Model (PMRM) Technical Committee

---

1a) TC NAME

OASIS Privacy Management Reference Model (PMRM) Technical Committee

1b) STATEMENT OF PURPOSE AND PROBLEM TO BE SOLVED

For purposes of this project, from a business and operational perspective, "data privacy" is defined to mean the assured, proper, and consistent collection, storage, processing, transmission, use, sharing, trans border transfer, retention and disposition of Personal Information (PI) throughout its life cycle, consistent with data protection principles, privacy and security policy requirements, and the preferences of the individual, where applicable.

The principal purpose of the PMRM TC will be to develop and articulate a Privacy Management Reference Model that describes a set of broadly-applicable data privacy and security requirements and a set of implementable Services and interactions for fulfilling those requirements.

Today, increased cross-border and cross-policy domain data flows, networked information processing, federated systems, application outsourcing, social networks, ubiquitous devices and cloud computing bring ever significant challenges, risk, and management complexity to privacy management.

However, business process engineers, IT analysts, architects, and developers do not have standards-based technical privacy and security frameworks or lifecycle reference models that can enable development and implementation of privacy and associated security requirements. Frequently, expressed as broad policy objectives (fair information practices and principles), these objectives are far removed from the rigorous requirements' expressions needed by business sponsors, business and system analysts, architects and developers.

Typical policy expressions provide little insight into how to actually implement such policies, presenting frustration for policymakers (who expect business systems to manage privacy and security rules) and design challenges for IT architects and solution developers (who have few models to guide their work). This becomes a greater problem in increasingly federated networks, systems and applications.

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

The purpose of the OASIS Privacy Management Reference Model is to aid in the design and implementation of operational privacy and security management systems.

The Reference Model is intended to serve 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 controls. The Reference Model will serve as an evaluation framework for implementations, but will not itself be an implementation. It is intended to be used as a tool or basis for development of further implementations and standards, which either currently exist or would be developed independently.

1c) SCOPE OF THE TC

The TC will accept as input the ISTPA Privacy Management Reference Model v2.0 - a structure for resolving privacy policy requirements into operational controls and implementations - developed by the International Security, Trust and Privacy Alliance (ISTPA). It is anticipated that this document will be contributed to the TC for further elaboration and standardization at OASIS.

The TC is open to submission of other relevant work and encourages submissions, particularly use cases appropriate for testing the lifecycle management aspects of the Reference Model.

The PMRM will:

· Define a set of operationally-focused privacy requirements which can serve as a reference for evaluating options for designing and implementing operational privacy controls. These requirements will constitute a useful working set of 'privacy guidelines', which can both serve as general guidance, and as a feature set against which the PMRM and any implementation can be tested.
· Define a structured format for describing privacy management Services, and identify categories of functions that may be used in defining and executing the Services.
· Define a set of privacy management Services to support and implement the privacy requirements at a functional level. These Services will include some capabilities that are typically implicit in privacy practices or principles (such as policy management or interaction), but that are necessary if information systems and processes are to be made privacy configurable and compliant.
· Establish an explicit relationship between security requirements and supporting security services (such as confidentiality, integrity and availability services) and the privacy management Services. Security services and standards are essential to secure Personal Information; therefore, each specific privacy management Service is expected to have its own security service requirements.

In order to refine the Privacy Management Reference Model, the TC may employ and refine use cases supplied by other OASIS TCs and external organizations. The TC may also consider hosting educational workshops and producing additional supporting materials such as 'best practices' documents.

Specification of the performance of any particular security service, mechanism or standard for the security of Personal Information is out of scope for this TC. The Reference Model, however, will consider the applicability and relationship of security services (confidentiality, including identity management, authentication and access controls; integrity; and availability) within the

Reference Model, since the Reference Model incorporates security as a component of privacy management services.

1d) A LIST OF DELIVERABLES AND PROJECTED COMPLETION DATES
The key deliverables are the OASIS Privacy Management Reference Model and one or more comprehensive Use Cases. Estimated completion date is 12 months after the formation of this TC.

- Privacy Management Reference Model: Define a set of operational privacy management Services. Each Service will consist of a set of syntactically-structured and logically related Functions that implement that Service. The Service/Function sets will be complete in the sense that all arbitrary but rational sets of privacy requirements (e.g., principles, practices, privacy legislation) can be re-defined in terms of the Services. In that sense, the Reference Model will provide the basis for a high-level system design, a privacy architecture, and a privacy management implementation that solves the given set of privacy requirements.

- One or more comprehensive Use Cases: From a number of initial candidates solicited from a cross-section of vertical industries and privacy-sensitive environments, the TC will select one or more Use Cases and apply the Privacy Management Reference Model to convert the Use Case requirements into a system design for an implementation. Ideally, the Use Cases will fully exploit the set of operational Services.

As part of the Use Case development, two additional items are applicable: • Selection of one or more formal methodologies for expressing Use Cases, and, • Profiles of the PMRM applied to selected specific environments (such as Cloud Computing, Health IT, e-Gov, and/or the Smart Grid) that could be used to derive architectures for implementing the PMRM.
Any additional deliverables will be produced after the main deliverables have been finalized. However, additional, representative use cases can be developed in parallel with the Reference Model.

1e) IPR MODE UNDER WHICH TC WILL OPERATE
This TC will operate under the Non-Assertion Mode of the OASIS IPR Policy.

1f) ANTICIPATED AUDIENCE OR USERS OF THE WORK
The PMRM audience includes, but is not limited to, privacy policy makers, privacy and security consultants, auditors, IT systems architects and designers of systems that collect, store, process, use, share, transport across borders, exchange, secure, retain or destroy Personal Information. In addition, other OASIS TCs and external organizations and standards bodies may find the PMRM useful in developing privacy management use cases in their context.

1g) LANGUAGE IN WHICH THE TC WILL CONDUCT BUSINESS
The TC will conduct its business in English.

2 (NON-NORMATIVE) INFORMATION REGARDING THE STARTUP OF THE TC:

2a) Similar or applicable work being done and level of liaison:
Since most prior work related to privacy management implementation focuses on specific aspects, like policy expression languages or security controls for privacy, the PMRM is unprecedented in defining privacy management services for an arbitrary set of privacy requirements.
The TC may elect to form liaisons as appropriate with relevant OASIS TCs and outside organizations, including:

- OASIS Blue Member Section (for Smart Grid projects)
- Other OASIS IDtrust Member Section TCs (for Use Cases) - SOA Reference Model TC (for service models)
- ISO/IEC JTC1 Subcommittee 27 – Information technology - Security techniques
- ITU-T Study Group 17 on Security
- ISO TC 68 Subcommittee 7 on Financial Services Data Privacy
- International Association of Privacy Professionals
- US SmartGrid Interoperability Program (SGIP) Cybersecurity Committee
- Healthcare Information Technology Standards Panel (HITSP): Security, Privacy and Infrastructure Domain Technical Committee
- Kantara Initiative
- Liaison with ISO SC27/WG5 (on identity management and privacy)
- A global de jure standards organization such as ITU or ISO/IEC JTC1

2b) First meeting:
Date: Wednesday, 8 September 2010
Time: 11:00AM EDT
Location (in person or by telephone): Telephone
Sponsor: ISTPA and CA Technologies

2c) Meeting schedule and Sponsor: Weekly teleconferences, time/date TBD, periodic face-to-face in conjunction with the OASIS IDtrust Member Section meetings; possible face-to-face meeting (with teleconference option) coincident with the OASIS Identity Management 2010 Conference, Washington, DC; sponsors: CA Technologies and ISTPA

2d) Names, electronic mail addresses, and membership affiliations of supporting Minimum Membership (proposers):
John Sabo, John.T.Sabo@ca.com, CA Technologies
Michael Willett, mwillett@nc.rr.com, ISTPA
Erika McCallister, Erika.mccallister@nist.gov, NIST
Rolly Chambers, RLChambers@smithcurrie.com, American Bar Association Bill Tabor, btabor@protexx.com, WidePoint Corporation
Peter Brown, peter-oasis@justbrown.net, (individual)
John Bradley, john.bradley@wingaa.com, (individual)
Michele Drgon, micheledrgon@dataprobity.com, (individual)
Gail Magnuson, gail.magnuson@gmail.com, (individual)

John Moehrke, John.Moehrke@med.ge.com, (individual)

2e) For each OASIS Organizational Member above, name, electronic mail address, membership affiliation, and statement of support

John Sabo, John.T.Sabo@ca.com
Director, Global Government Relations
CA Technologies and President: ISTPA

As the Primary Representative to OASIS of the International Security, Trust, and Privacy Alliance (ISTPA), I approve the Charter. ISTPA is pleased to be able to contribute our Privacy Management Reference Model v2.0 to the technical committee. We believe that the new PMRM TC will undertake important standardization work in lifecycle privacy management and compliance. --
Rolly Chambers, RLChambers@smithcurrie.com, American Bar Association
I'm assuming you realize the ABA approves.
--
Paul Lipton, paul.lipton@ca.com
VP, Industry Standards and Open Source, CA Technologies

As CA Primary Representative, I approve the PMRM TC Charter and CA's inclusion (in the person of John Sabo) as a named co-proposer. Also, my compliments on the quality of the charter itself. It has come along nicely, if I may be so bold.
--
David Flater, dflater@nist.gov
National Institute of Standards and Technology

As the NIST primary representative to OASIS, I approve the final draft of the PMRM TC charter.
--
Bill Tabor, btabor@protexx.com WidePoint

I am the Primary Rep for Widepoint and I approve.
--

2f) Convener:
Michael Willett

2g) Member Section: IDtrust

2h) Contributions of existing technical work:
ISTPA Privacy Management Reference Model V2.0:
http://www.istpa.org/pdfs/ISTPAPrivacyManagementReferenceModelV2%200.pdf

2i) Draft Frequently Asked Questions (FAQ) document: TBD (Willett)
2j) Proposed working title and acronym for the specification(s): OASIS Privacy Management

Reference Model (PMRM), pronounced ‘pimrim’.