SAINT MARY'S UNIVERSITY
SOBEY
SCHOOL OF BUSINESS

Privacy by Design Documentation for Software Engineers (PbD-SE TC)

Dawn N. Jutla , PhD, Director, Board of OASIS
Professor of Computer Science and Business, Sobey School of Business, Saint Mary's University
Convener and co-Chair/co-editor, OASIS PbD-SE TC with Commissioner Ann Cavoukian; co-editor, OASIS PMRM

May 13, 2014
European Identity and Cloud Conference

@ OASIS
Advancing open standards for the information society

PbD

SAINT MARY'S UNIVERSITY
SOBEY
SCHOOL OF BUSINESS

EMERGING Standards to make **Privacy-by-Design Instinctual** on the **Internet**

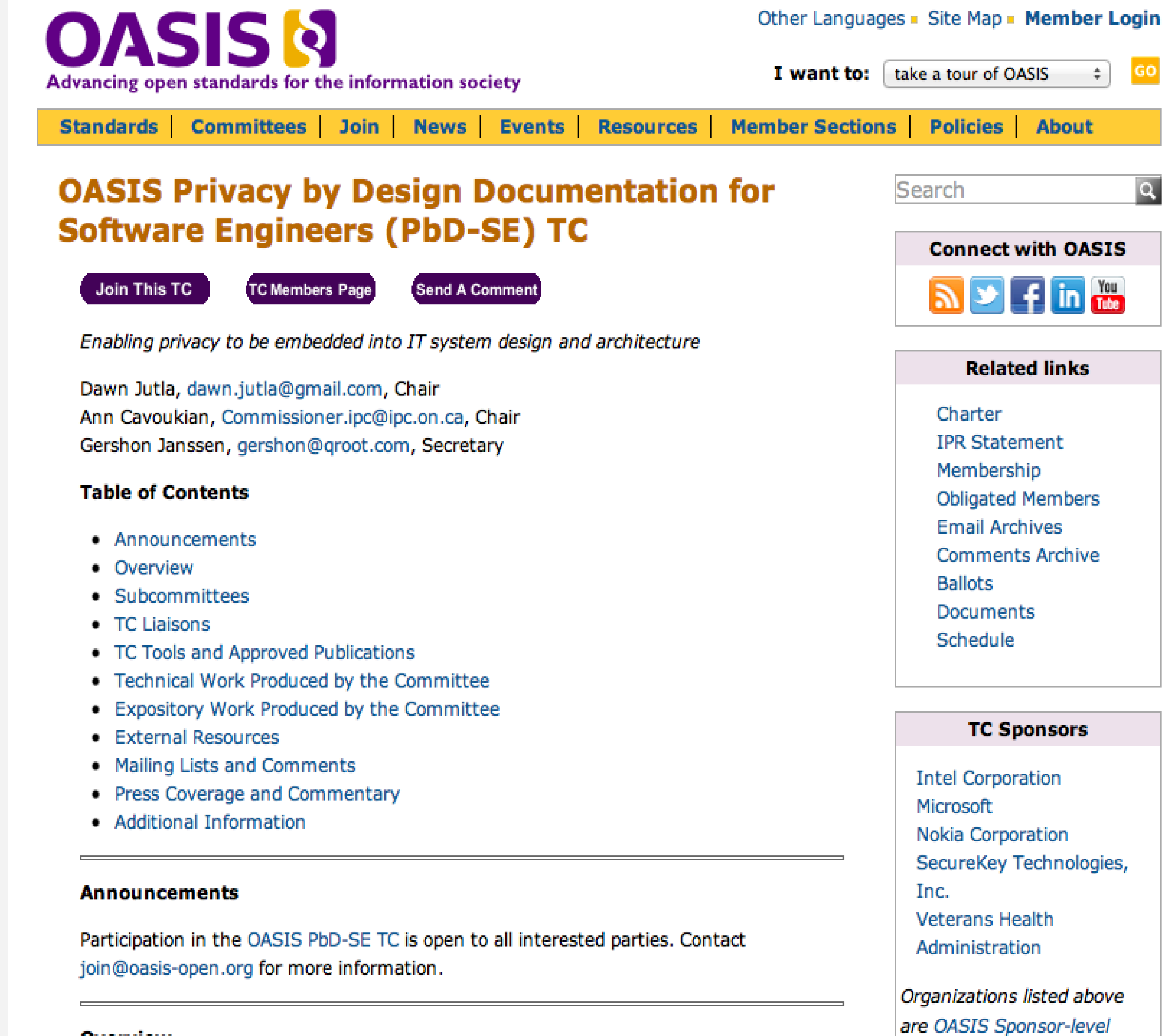
FOR EVERY ORGANIZATION AND SOFTWARE ENGINEER – ON PURPOSE, IN A MANAGED WAY

OASIS
Advancing open standards for the information society

GARTNER 2014 PREDICTS:

By 2017, 80% of consumers will
collect, track and barter
their personal data for cost savings,
convenience and customization.

OASIS PbD-SE



OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC

Enabling privacy to be embedded into IT system design and architecture

Dawn Jutla, dawn.jutla@gmail.com, Chair
Ann Cavoukian, Commissioner.ipc@ipc.on.ca, Chair
Gershon Janssen, gershon@qroot.com, Secretary

Table of Contents

Announcements

Participation in the OASIS PbD-SE TC is open to all interested parties. Contact join@oasis-open.org for more information.

Connect with OASIS

Related links

- Charter
- IPR Statement
- Membership
- Obligated Members
- Email Archives
- Comments Archive
- Ballots
- Documents
- Schedule

TC Sponsors

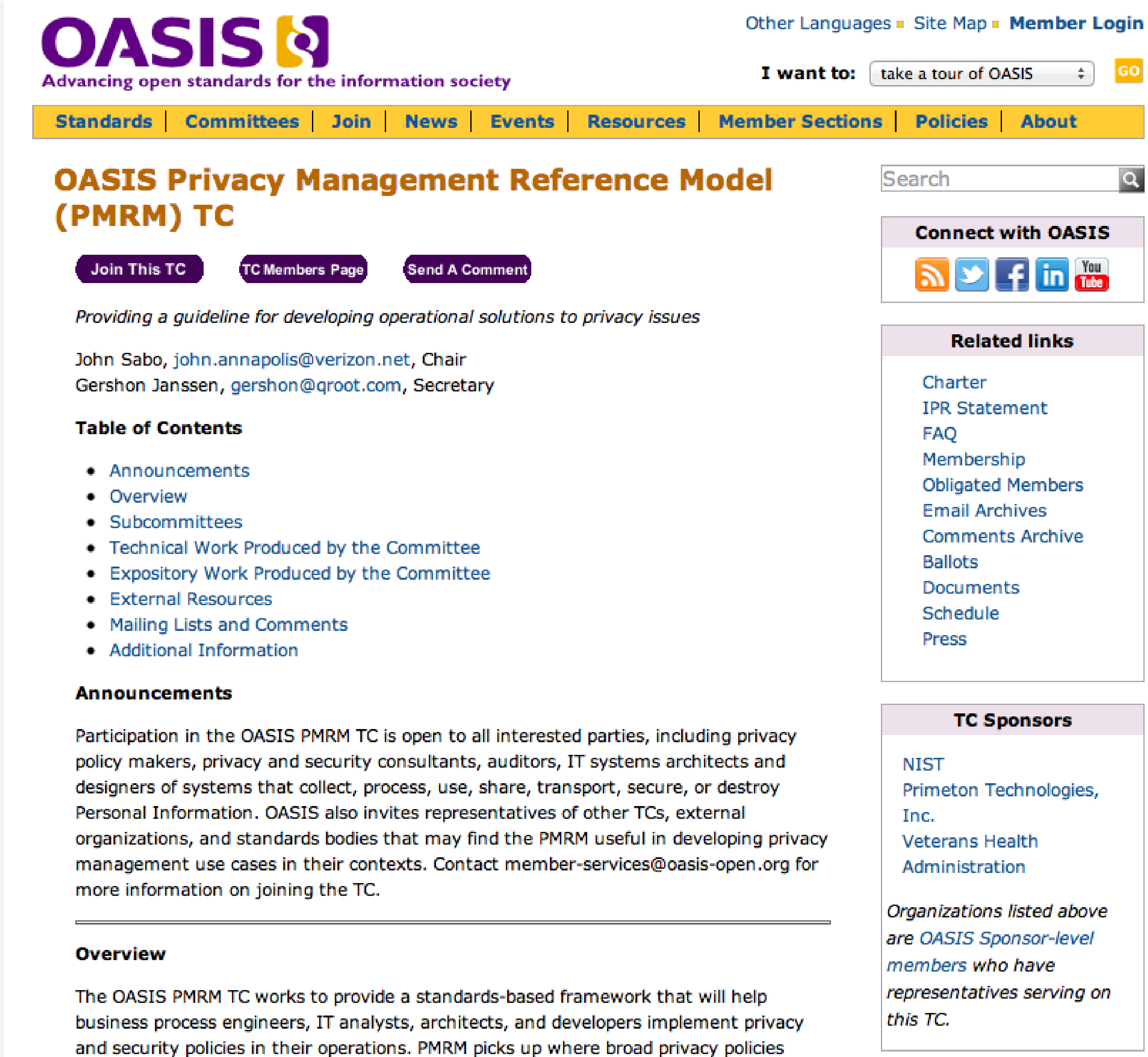
Intel Corporation
Microsoft
Nokia Corporation
SecureKey Technologies, Inc.
Veterans Health Administration

Organizations listed above are OASIS Sponsor-level

Why should business care …
about consumer privacy & empowerment over personal data?

- Loss of customers, customer loyalty, stock value, and brand reputation
- Increased legal costs, class action lawsuits
- Shareholder and board dissatisfaction

OASIS PMRM


OASIS
Advancing open standards for the information society
Other Languages ▪ Site Map ▪ Member Login
I want to: take a tour of OASIS
GO
Standards | Committees | Join | News | Events | Resources | Member Sections | Policies | About
Search
Join This TC
TC Members Page
Send A Comment

OASIS Privacy Management Reference Model (PMRM) TC

Providing a guideline for developing operational solutions to privacy issues

John Sabo, john.annapolis@verizon.net, Chair
Gershon Janssen, gershon@qroot.com, Secretary

Table of Contents

Announcements

Participation in the OASIS PMRM TC is open to all interested parties, including privacy policy makers, privacy and security consultants, auditors, IT systems architects and designers of systems that collect, process, use, share, transport, secure, or destroy Personal Information. OASIS also invites representatives of other TCs, external organizations, and standards bodies that may find the PMRM useful in developing privacy management use cases in their contexts. Contact member-services@oasis-open.org for more information on joining the TC.

Overview

The OASIS PMRM TC works to provide a standards-based framework that will help business process engineers, IT analysts, architects, and developers implement privacy and security policies in their operations. PMRM picks up where broad privacy policies

Connect with OASIS

Related links

Charter
IPR Statement
FAQ
Membership
Obligated Members
Email Archives
Comments Archive
Ballots
Documents
Schedule
Press

TC Sponsors

NIST
Primeton Technologies, Inc.
Veterans Health Administration

Organizations listed above are OASIS Sponsor-level members who have representatives serving on this TC.

OASIS

OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC

1 PbD principles are internationally recognized with mappings/alignment to FIPPs, GAPPs and NIST 800-53 Appendix J controls.

2 Help stakeholders to **visualize** privacy requirements and design from software conception to retirement

3 A specification of a methodology, mappings, and guidance to help software engineers to :

- Model and translate Privacy by Design (PbD) principles to conformance requirements within software engineering tasks,
- Produce privacy-aware software, and document artifacts as evidence of PbD-principle compliance.
- Collaborate with management and auditors to *simplify* demonstration of compliance/audits.

OASIS Privacy Management Reference Model and Methodology (PMRM) Emerging Standard

TC Chair: John T. Sabo

1 PMRM provides a model and methodology for translating & mapping privacy requirements,, as the basis for a PRIVACY SERVICE ARCHITECTURE: http://j.mp/oasisPMRM

2 KEY STRENGTH: Gets at how personal data flow among data platforms... 360 stakeholder view of privacy requirements. Considers context!

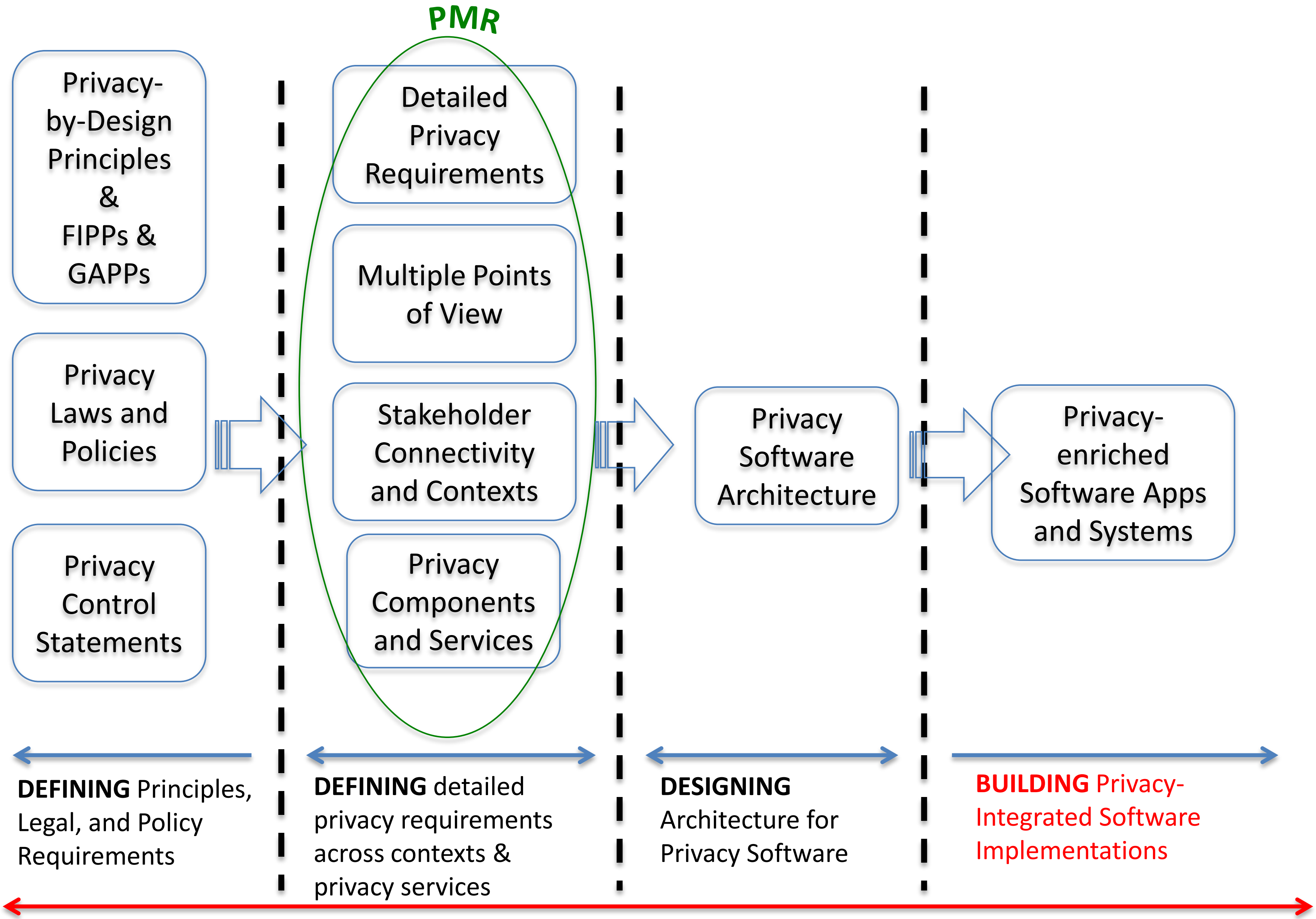
3 Major elements of this emerging standard's methodology and the PbD-SE methodology unify and align with the state-of-the-art in the:

- Dennedy, Finneran, and Fox's Privacy Engineering Manifesto book (industry-led – McAfee)
- Shostack's Threat Modeling book (industry led- Microsoft)
- Content in the Privacy Engineering program at Carnegie Mellon and extant privacy literature (university-led)

OASIS

Advancing open standards for the information society

Scope of the OASIS PbD-SE and OASIS PMRM Standard-Track Work Products



PMR

Privacy-by-Design Principles & FIPPs & GAPPs

Privacy Laws and Policies

Privacy Control Statements

Detailed Privacy Requirements

Multiple Points of View

Stakeholder Connectivity and Contexts

Privacy Components and Services

Privacy Software Architecture

Privacy-enriched Software Apps and Systems

DEFINING Principles, Legal, and Policy Requirements

DEFINING detailed privacy requirements across contexts & privacy services

DESIGNING Architecture for Privacy Software

BUILDING Privacy-Integrated Software Implementations

OASIS PbD-SE crosses the entire 4-stage spectrum from principles to implementation

Applicable to all organizations and individuals producing Information Technology Products and Services

Software Engineer: A person that adopts engineering approaches, such as established methodologies, processes, architectures, measurement tools, standards, organization methods, management methods, quality assurance systems and the like, in the development of large scale software, seeking to result in high productivity, low cost, controllable quality, and measurable development schedule.

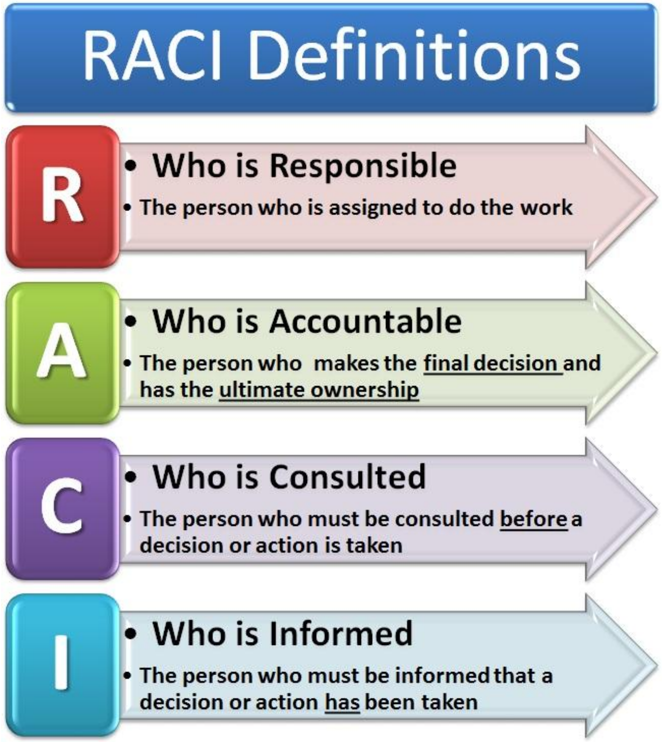
Source: Adapted from Y. Wang, Senior Member of the IEEE and ACM. Theoretical Foundations of Software Engineering, Schulich School of Engineering, University of Calgary, 2011.

Large scale software extends to include apps that scale to millions of users

Organizations and individuals adopting design processes, privacy methodologies, models, and standards to obtain better user privacy going forward.

OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC

RACI Chart for OASIS PbD-SE Methodology (WIP)



RACI Definitions

R – Who is Responsible
- The person who is assigned to do the work

A – Who is Accountable
- The person who makes the final decision and has the ultimate ownership

C – Who is Consulted
- The person who must be consulted before a decision or action is taken

I – Who is Informed
- The person who must be informed that a decision or action has been taken

PbD-SE Methodology Step	Documented Activity	Software Engineer	Privacy Resource	Project Mgmt.	Mgmt.	Third Party	User
3.1 Assess Organization-al Readiness	Document Privacy Policy Document	CI	RA CI	CI	A CI	I	CI
	Document Privacy Roles/Training Program in Organization	I	RA CI	CI	A I	I	I
3.2 Scope Privacy Requirements & Reference Architecture	Document Functional Privacy Requirements & hooks to Reference Architecture	RA	RA CI	ACI	A I	RA I	CI
3.3 Conduct Risk Analysis on Use Cases	Document Business Model with Personal Data Flows	CI	RA CI	CI	A C	CI	-
	Document Risk analysis (incl. threat models, PIA)	CI	RA CI	CI	A CI	CI	-
3.4 Identify Privacy Resource Allocation	Document privacy resource allocation to SE team	I	RACI	RI	A I	I	-
3.5 Create RACI for Producing Artifacts	Document RACI assignment to artifact production	RCI	CI	RA CI	A I	-	-
3.6 Customize Privacy Architecture	Document Privacy Architecture	RA	A CI	A CI	A I	I	-
3.7 Conduct Periodic Review	Document Review of Artifacts throughout the PDLC	RA	CI	RA CI	A I	-	-
3.8 Execute Code Testing & Privacy Evaluation	Document testing and evaluation for satisfying privacy properties	RA	RCI	RA CI	A I	-	C
3.9 Create Retirement Plan	Document plan for retirement of software solution	CI	RA CI	RA CI	A CI	I	I
3.10 Sign-off	Document sign off with checklist	RA CI	RA CI	RA CI	A C	-	-

PbD “Sub-Principles”	*Documentation*
1. *Proactive* not Reactive; *Preventative* not Remedial	
1.1–Demonstrable Leadership: A clear commitment, at the highest levels, to prescribe and enforce high standards of privacy protection, generally higher than prevailing legal requirements. **1.2–Defined Community of Practice**: Demonstrable privacy commitment shared by organization members, user communities and stakeholders. **1.3–Proactive and iterative**: Continuous processes to identify privacy and data protection risks arising from poor designs, practices and outcomes, and to mitigate unintended or negative impacts in proactive and systematic ways	**MUST** normatively reference the PbD-SE specification **MUST** reference assignment of responsibility and accountability for privacy in the organization, and privacy training program. **MUST** include assignment of privacy resources to the software project, recording who are responsible, accountable, consulted, or informed for various privacy-related tasks **MUST** reference all external sources of privacy requirements, including policies, principles, and regulations. **MUST** include privacy requirements specific to the service/product being engineered, and anticipated deployment environments **MUST** include privacy risk/threat model(s) including analysis and risk identification, risk prioritization, and controls clearly mapped to risks

PbD "Sub-Principles"	*Documentation*
2. Privacy by Default	
2.1–Purpose Specificity: Purposes must be specific and limited, and be amenable to engineering controls **2.2–Adherence to Purposes:** methods must be in place to ensure that personal data is collected, used and disclosed: in conformity with specific, limited purposes; in agreement with data subject consent; and in compliance with applicable laws and regulations **2.3–Engineering Controls:** Strict limits should be placed on each phase of data processing lifecycle engaged by the software under development, including: Limiting Collection; Collecting by Fair and Lawful Means; Collecting from Third Parties; Limiting Uses and Disclosures; Limiting Retention; Disposal, Destruction; and Redaction	**SHOULD** list all [categories of] data subjects as a stakeholder **MUST** document expressive traceable models of detailed data flows, processes, behaviors, and the privacy properties to be satisfied for the use cases or user stories associated with internal software project and all data/process interaction with external platforms, systems, APIs, and/or imported code. (Examples of expressive models are roughly *equivalent* to UML models) **MUST** describe selection of privacy controls and privacy services/APIs and where they apply to privacy functional requirements and risks. **MUST** include software retirement plan from a privacy viewpoint

PbD "Sub-Principles"	*Documentation*
3. Privacy embedded in design	
3.1–Holistic and Integrative: Privacy commitments must be embedded in holistic and integrative ways **3.2–Systematic and Auditable:** A systematic, principled approach should be adopted that relies upon accepted standards and process frameworks, and is amenable to external review. **3.3–Review and Assess:** Detailed privacy impact and risk assessments should be used as a basis for design decisions. **3.4–Human-Proof:** The privacy risks should be demonstrably minimized and not increase through use, misconfiguration, or error.	The OASIS PMRM Privacy Use Case Template is **RECOMMENDED** as a tool to use for iterating and identifying and documenting privacy requirements and assessment. **MUST** contain description of business model showing traceability of personal data flows for any data collected through new software services under development. **MUST** include identification of the privacy properties that inform software design **MUST** contain a privacy architecture that satisfies system-level and user-level privacy properties **MUST** detail privacy UI/UX design **MUST** define privacy metrics **MUST** include human sign-offs/privacy checklists for software engineering artifacts **MUST** include privacy review reports *(either in reviewed documents or in separate report)*

PbD "Sub-Principles"	*Documentation*
4. Full Functionality: Positive Sum, not Zero-Sum	
4.1–No Loss of Functionality: Embedding privacy adds to the desired functionality of a given technology, process or network architecture. **4.2-Accommodate Legitimate Objectives**: All interests and objectives must be documented, desired functions articulated, metrics agreed, and trade-offs rejected, when seeking a solution that enables multi-functionality **4.3–Practical and Demonstrable Results**: Optimized outcomes should be published for others to emulate and become best practice	**MUST** treat *privacy-as-a-functional requirement,* i.e. functional software requirements and privacy requirements should be considered together, with no loss of functionality. **MUST** show tests for meeting privacy objectives, in terms of the operation and effectiveness of implemented privacy controls or services. MUST show the integration of, or hooks between, functional privacy architecture and functional software architecture.

PbD “Sub-Principles”	*Documentation*
5. End-to-End Lifecycle Protection	
5.1–Protect Continuously: Personal data must be continuously protected across the entire domain and throughout the data life-cycle from creation to destruction	**MUST** be produced for all stages of the software development lifecycle from referencing applicable principles, policies, and regulations to defining privacy requirements, to design, implementation, maintenance, and retirement.
5.2–Control Access: Access to personal data should be commensurate with its degree of sensitivity, and be consistent with recognized standards and criteria	**MUST** reference requirements, risk analyses, architectures, design, implementation mechanisms, retirement plan, and sign-offs with respect to privacy and security.
5.3–Use Security and Privacy Metrics: Applied security standards must assure the confidentiality, integrity and availability of personal data and be amenable to verification Applied privacy standards must assure user/data subject comprehension, choice, consent, consciousness, consistency, confinement (setting limits to collection, use, disclosure, retention, purpose), and context(s) around personal data at a functional level, traceability of data flows, and minimized identifiability, linkability, and observability at a systems level, and be amenable to verification	**MUST** reference security AND privacy properties and metrics designed and/or deployed by the software, or monitoring software, or otherwise in the organization and across partnering software systems or organizations.

OASIS Privacy by Design Documentation for
Software Engineers (PbD-SE) TC

PbD “Sub-Principles”	*Documentation*
6. Visibility and Transparency	
6.1–Open Collaboration: Privacy requirements, risks, implementation methods and outcomes should be documented throughout the development lifecycle and communicated to project members and stakeholders. **6.2–Open to Review:** The design and operation of software systems should demonstrably satisfy the strongest privacy laws, contracts, policies and norms (as required). **6.3–Open to Emulation:** The design and operation of privacy-enhanced information technologies and systems should be open to scrutiny, improvement, praise, and emulation by all.	**MUST** *reference* the privacy policies and documentation of all other collaborating stakeholders **MUST** include description of contextual visibility and transparency mechanisms at the point of contextual interaction with the data subject (user) and other stakeholders for data collection, use, disclosure, and/or elsewhere as applicable **MUST** describe any measurements incorporated in the software, or monitoring software, or otherwise to measure the usage and effectiveness of provided privacy options and controls, and to ensure continuous improvement. **MUST** describe placement of privacy settings, privacy controls, privacy policy(ies), and accessibility, prominence, clarity, and intended effectiveness.

PbD “Sub-Principles”	*Documentation*
7. Respect for User Privacy	
7.1–Anticipate and Inform: Software should be designed with user/data subject privacy interests in mind, and convey privacy attributes (where relevant) in a timely, useful, and effective way. **7.2–Support Data Subject Input and Direction:** Technologies, operations and networks should allow users/data subjects to express privacy preferences and controls in a persistent and effective way. **7.3–Encourage Direct User/Subject Access:** Software systems should be designed to provide data subjects direct access to data held about them, and an account of uses and disclosures.	**MUST** describe user privacy options (including access), controls, user privacy preferences/settings, UI/UX supports, and user-centric privacy model. **MUST** describe notice, consent, and other privacy interactions at the EARLIEST possible point in a data transaction exchange with a user/data subject or her/his automated agent(s) or device(s).

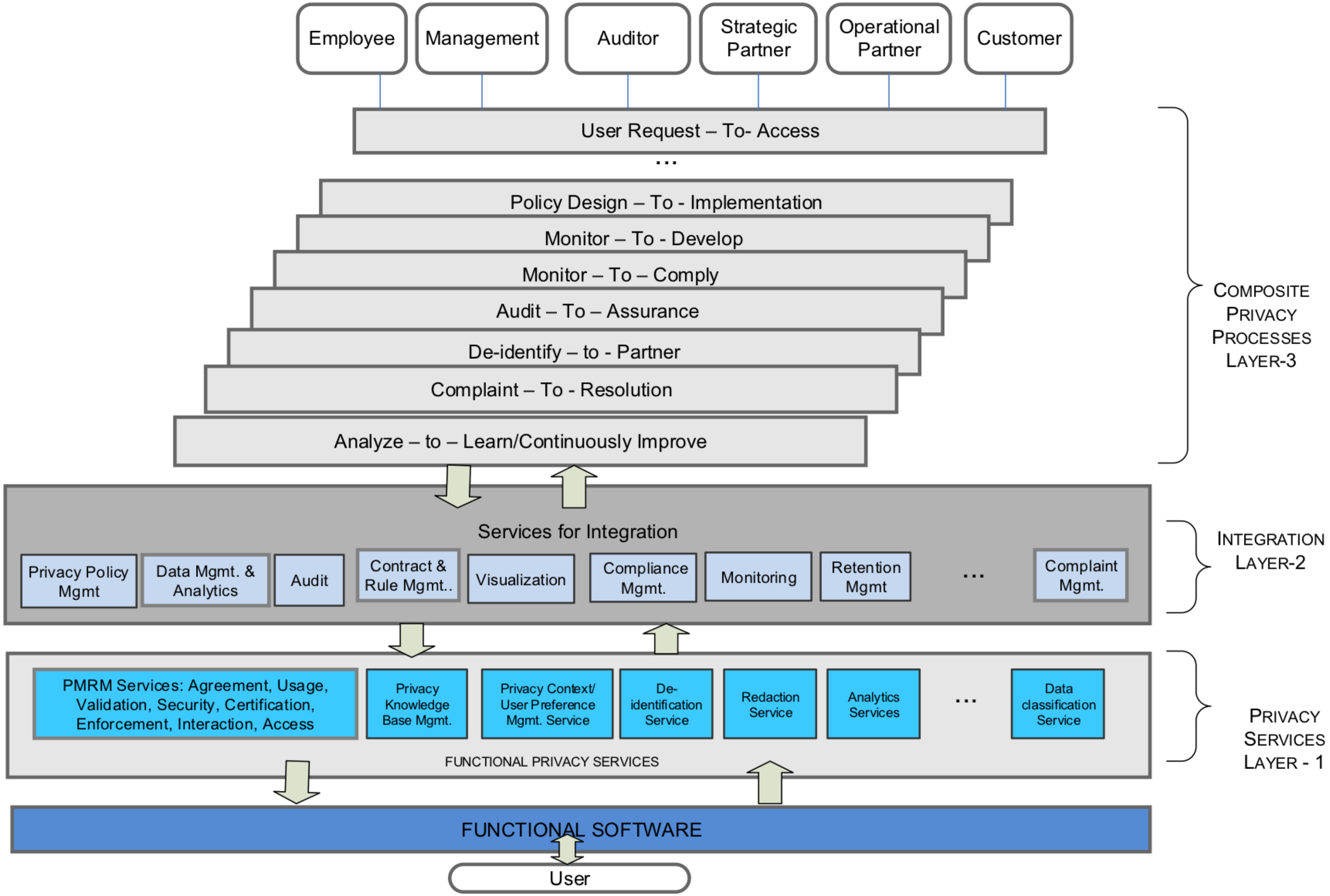
TOILING the 7Cs: Privacy Properties as a Basis for Architectural Requirements

Comprehension **(User understanding of how PII is handled)**	**Users should *understand* how personal identifiable information (PII) is handled, who's collecting it and for what purpose, and who will process the PII and for what purpose across software platforms. Users are entitled to visibility to know all parties that can access their PII, how to access/correct their own data, the limits to processing transparency, why the PII data is being requested, when the data will expire (either from a collection or database), and what happens to it after that. This category also includes legal rights around PII, and the implications of a contract when one is formed.**
Consciousness **(User awareness of what is happening and when)**	Users should be *aware* of when data collection occurs, when a contract is being formed between a user and a data collector, when their PII is set to expire, who's collecting the data, with whom the data will be shared, how to subsequently access the PII, and the purposes for which the data is being collected.
Choice **(To opt-in or out, divulge or refuse to share PII)**	Users should have *choices* regarding data collection activities in terms of opting in or out, whether or not to provide data, and how to correct their data.
Consent **(Informed, explicit, unambiguous)**	Users must first consent (meaning informed, explicit, unambiguous agreement) to data collection, use, and storage proposals for any PII. Privacy consent mechanisms should explicitly incorporate mechanisms of comprehension, consciousness, limitations, and choice.
Context **(User adjusting preferences as conditions require)**	Users should/must be able to *change privacy preferences* according to context. Situational or physical context—such as crowded situations (for example, when at a service desk where several people can listen in on your exchange when you provide a phone number, or when you are in the subway with cameras and audio on wearables around you)—is different from when you perform a buy transaction with Amazon.com or provide information to an app registered with an aggregator that sells to advertisers. Data also has context (such as the sensitivity of data, for example, financial and health data) could dictate different actions on the same PII in different contexts.
Confinement **(Data minimization, proportionality, and user-controlled re-use of data)**	Users must/should be able to *set/request limits* on who may access their PII, for what purposes, and where and possibly when/how long it may be stored. Setting limits could provide some good opportunities for future negotiation between vendors and users.
Consistency **(User predictability of outcome of transactions)**	Users should *anticipate with reasonable certainty* what will occur if any action i their PII is taken. That is, certain actions should be predictable on user access of giving out of PII.

T – Traceability
O - Observability
I – Identifiability
Linkability – measure of the degree that a real identity can be linked to data (BIRO, 2009)

Adapted from: Dawn N. Jutla, Peter Bodorik, "Sociotechnical Architecture for Online Privacy," IEEE Security and Privacy, vol. 3, no. 2, pp. 29-39, March-April 2005, doi:10.1109/MSP.2005.50. http://bit.ly/1qePUpn

PRIVACY ARCHITECTURAL BLUEPRINT



Employee
Management
Auditor
Strategic Partner
Operational Partner
Customer
User Request – To- Access
…
Policy Design – To - Implementation
Monitor – To - Develop
Monitor – To – Comply
Audit – To – Assurance
De-identify – to - Partner
Complaint – To - Resolution
Analyze – to – Learn/Continuously Improve
Composite Privacy Processes Layer-3
Services for Integration
Privacy Policy Mgmt
Data Mgmt. & Analytics
Audit
Contract & Rule Mgmt..
Visualization
Compliance Mgmt.
Monitoring
Retention Mgmt
…
Complaint Mgmt.
Integration Layer-2
PMRM Services: Agreement, Usage, Validation, Security, Certification, Enforcement, Interaction, Access
Privacy Knowledge Base Mgmt.
Privacy Context/ User Preference Mgmt. Service
De-identification Service
Redaction Service
Analytics Services
…
Data classification Service
FUNCTIONAL PRIVACY SERVICES
Privacy Services Layer - 1
FUNCTIONAL SOFTWARE
User

The Software Engineers' 1000 word models: Example Representations for Documentation

OASIS

OASIS Privacy by Design Documentation for
Software Engineers (PbD-SE) TC

Spreadsheets

- Columns
  - Description of Personal Data/Data Cluster
  - Personal Info Category
  - PII Classification
  - Source
  - Collected by
  - Collection Method
  - Type of Format
  - Used By
  - Purpose of Collection
  - Transfer to De-Identification
  - Security Control during Data Transfer
  - Data Repository Format
  - Storage or data retention site
  - Disclosed to
  - Retention Policy
  - Deletion Policy
- DFDs
- Compare design options (identifiab-ility, linkab-ility, observab-ility)

4

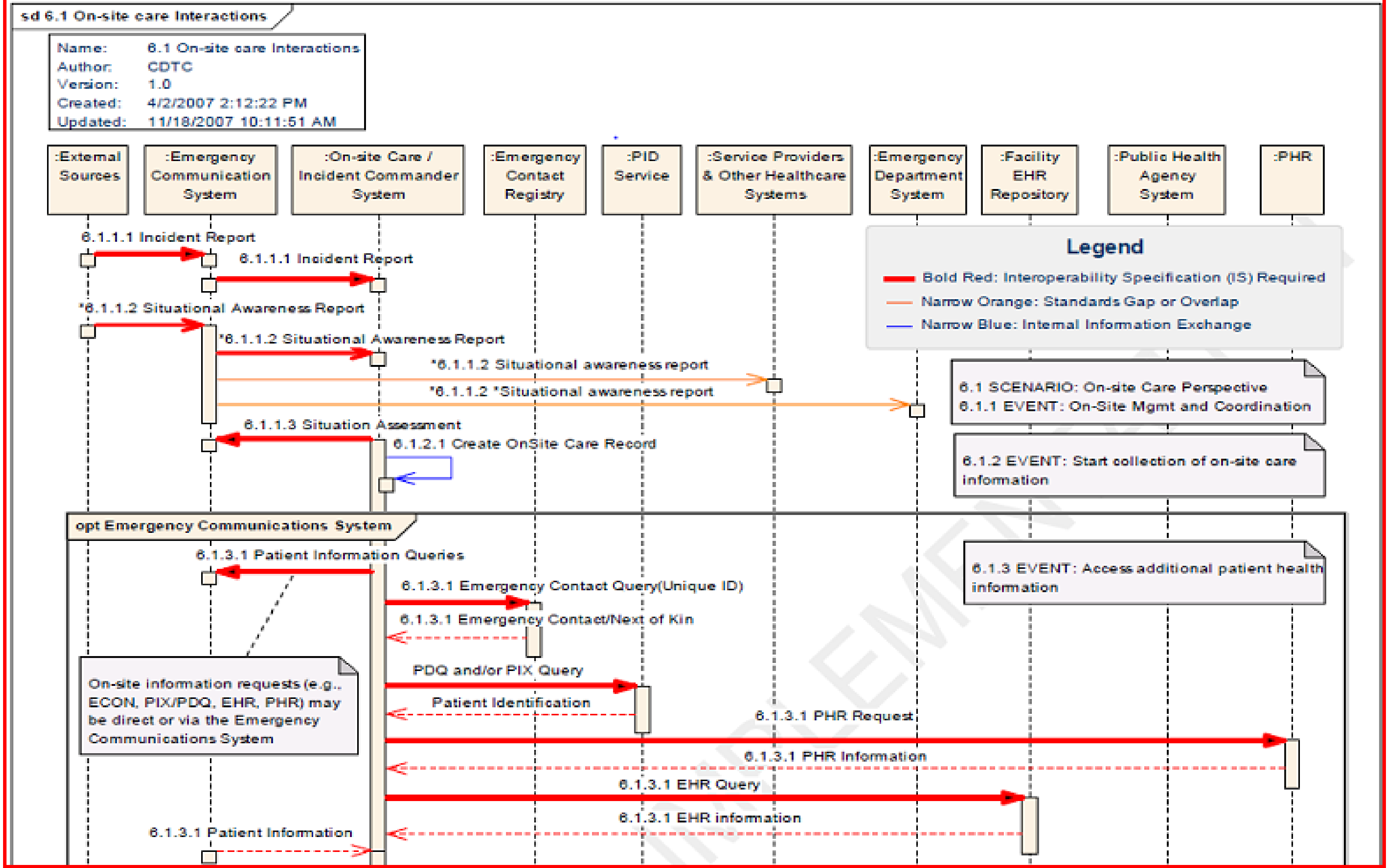
OASIS PMRM Methodology Step: For each actor instance, and incoming/outcoming data flow within a use case instance, (a) add context to requirements, and (b) determine the PMRM Services

Table 1. Data Flows TO a Single Actor with PMRM Service Invocations.

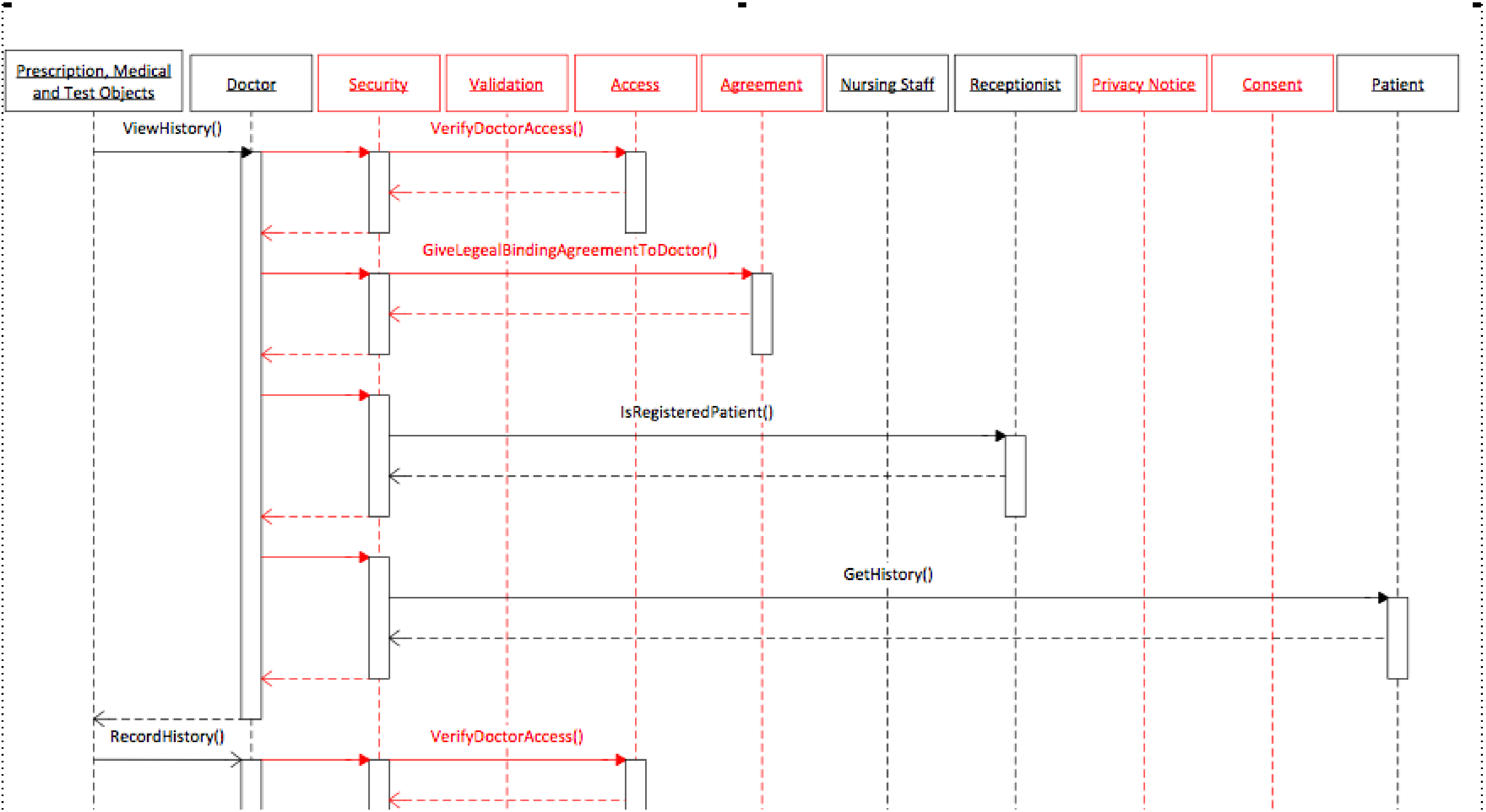
ACTOR:	PI-In	Actor Source	Requirements	PMRM SVCs	[Context Narrative]	Comment
ECS	Incoming Data Flows		[Examples – Qualify with Context]			
	Incident Report	External sources	• ECS Privacy and Security Policy • jurisdictional regulations • OnStar	• Security • Control • Audit • Interaction • Validation • Usage	Incident involving Californians with all health info within the City of Sacramento	Data elements require further definition
	Situational Awareness Report	External Sources	• ECS Privacy and Security Policy • jurisdictional regulations • OnStar	• Security • Control • Audit • Interaction • Validation • Usage		
	Patient EHR Information	Service Provider and other Healthcare systems	• HIPAA security and privacy rules • HITECH • 3rd party inherited policy agreements	• Security • Control • Audit • Interaction • Validation • Certification • Usage		If Individual access or enforcement are necessary to the ECS, then Access and enforcement services required
	Situation Assessment	On-site Care/Incident Commander	• General scene information	• None		

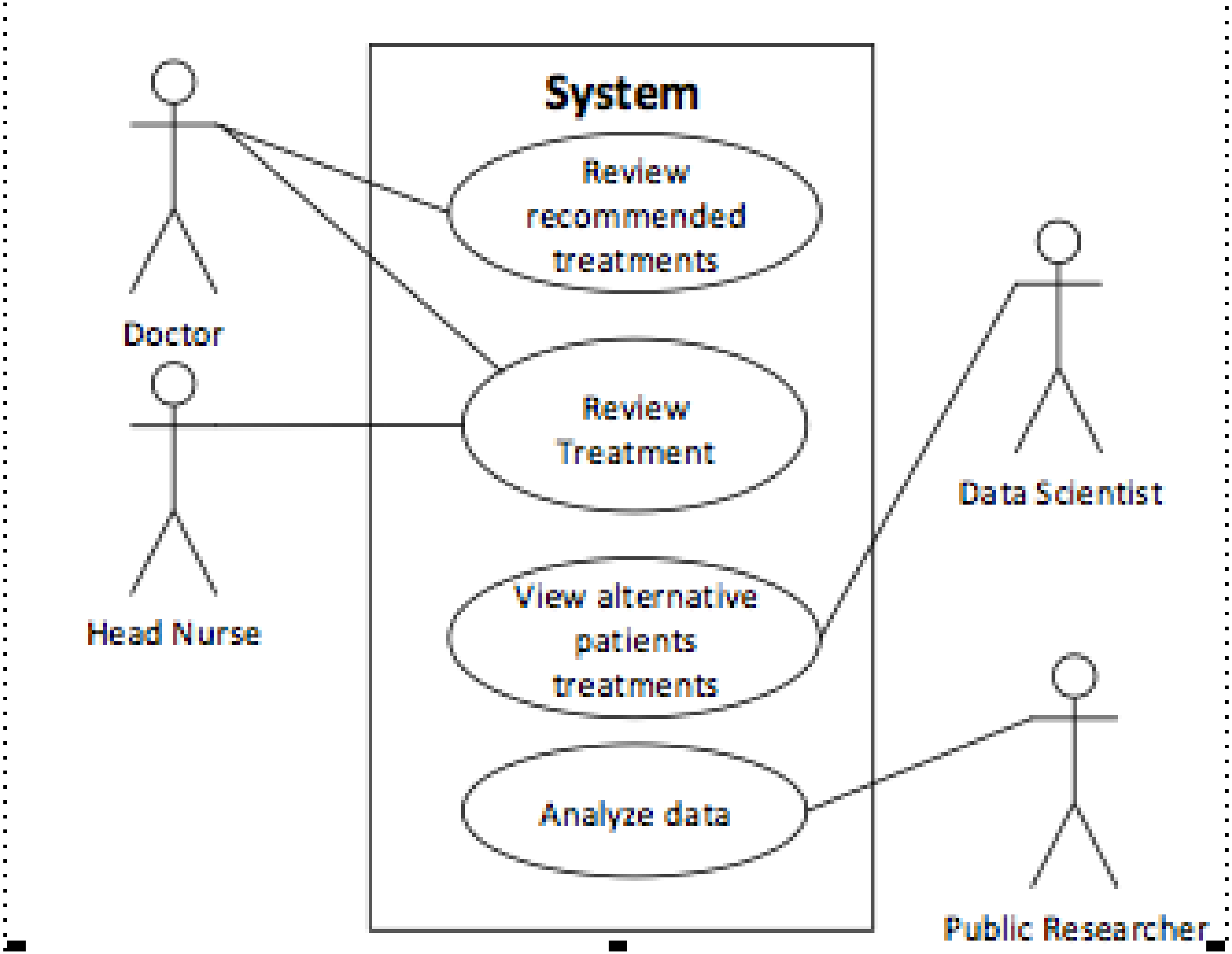
OASIS PMRM & PbD-SE Methodology Step: Describe the business processes and data flows using a data lifecycle description model and provide the level of detail needed to include <u>all actors and touch points</u>

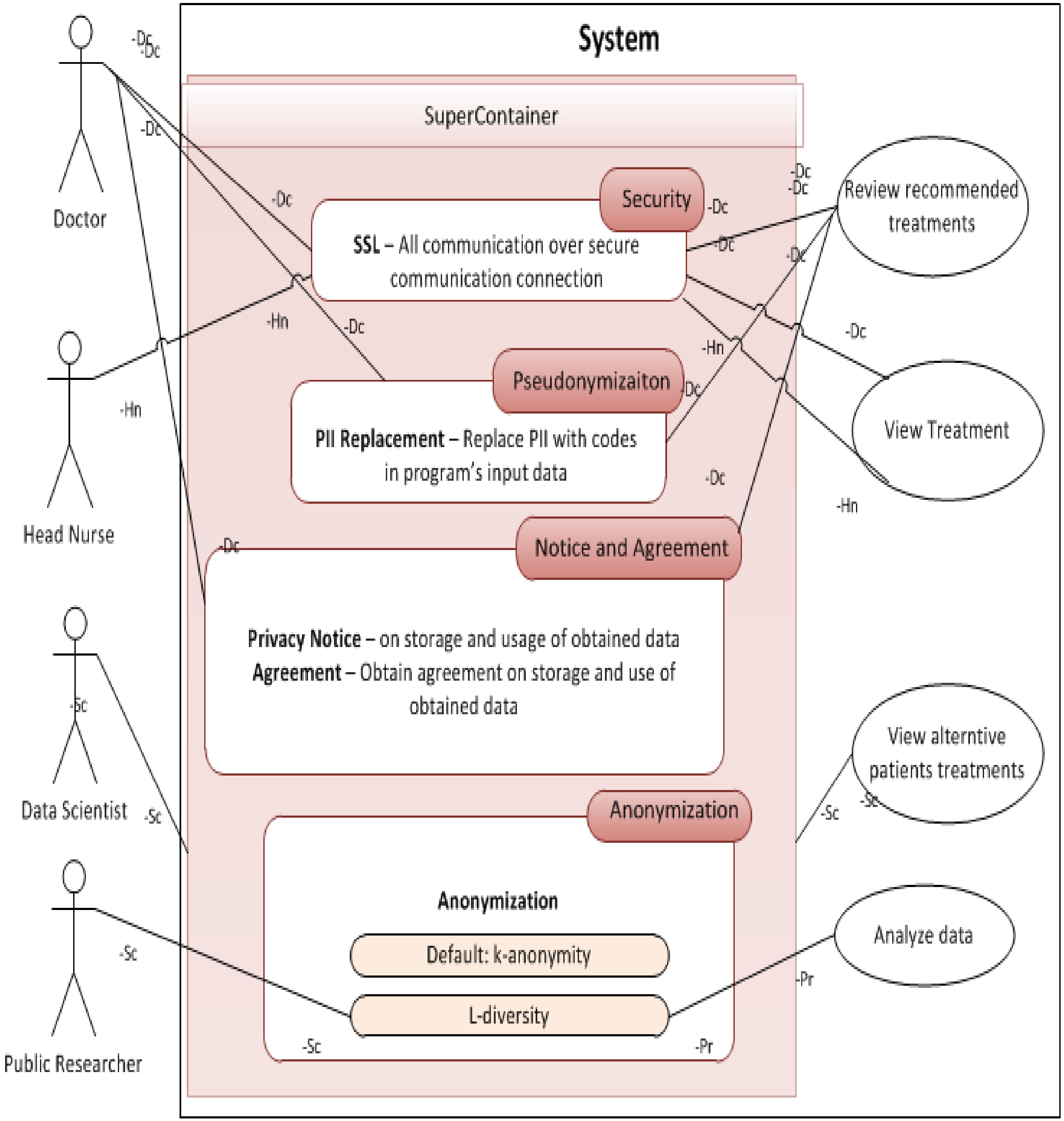
Figure 2.2.4.1-1 On-Site Care Scenario Perspective Business Sequence Diagram


sd 6.1 On-site care Interactions
Name: 6.1 On-site care Interactions
Author: CDTC
Version: 1.0
Created: 4/2/2007 2:12:22 PM
Updated: 11/18/2007 10:11:51 AM
:External Sources
:Emergency Communication System
:On-site Care / Incident Commander System
:Emergency Contact Registry
:PID Service
:Service Providers & Other Healthcare Systems
:Emergency Department System
:Facility EHR Repository
:Public Health Agency System
:PHR
Legend
Bold Red: Interoperability Specification (IS) Required
Narrow Orange: Standards Gap or Overlap
Narrow Blue: Internal Information Exchange
6.1.1.1 Incident Report
6.1.1.1 Incident Report
*6.1.1.2 Situational Awareness Report
*6.1.1.2 Situational Awareness Report
*6.1.1.2 Situational awareness report
*6.1.1.2 *Situational awareness report
6.1 SCENARIO: On-site Care Perspective
6.1.1 EVENT: On-Site Mgmt and Coordination
6.1.1.3 Situation Assessment
6.1.2.1 Create OnSite Care Record
6.1.2 EVENT: Start collection of on-site care information
opt Emergency Communications System
6.1.3.1 Patient Information Queries
6.1.3 EVENT: Access additional patient health information
6.1.3.1 Emergency Contact Query(Unique ID)
6.1.3.1 Emergency Contact/Next of Kin
PDQ and/or PIX Query
Patient Identification
On-site information requests (e.g.. ECON, PIX/PDQ, EHR, PHR) may be direct or via the Emergency Communications System
6.1.3.1 PHR Request
6.1.3.1 PHR Information
6.1.3.1 EHR Query
6.1.3.1 EHR information
6.1.3.1 Patient Information

Visualizing Privacy Services in a UML Sequence Diagram



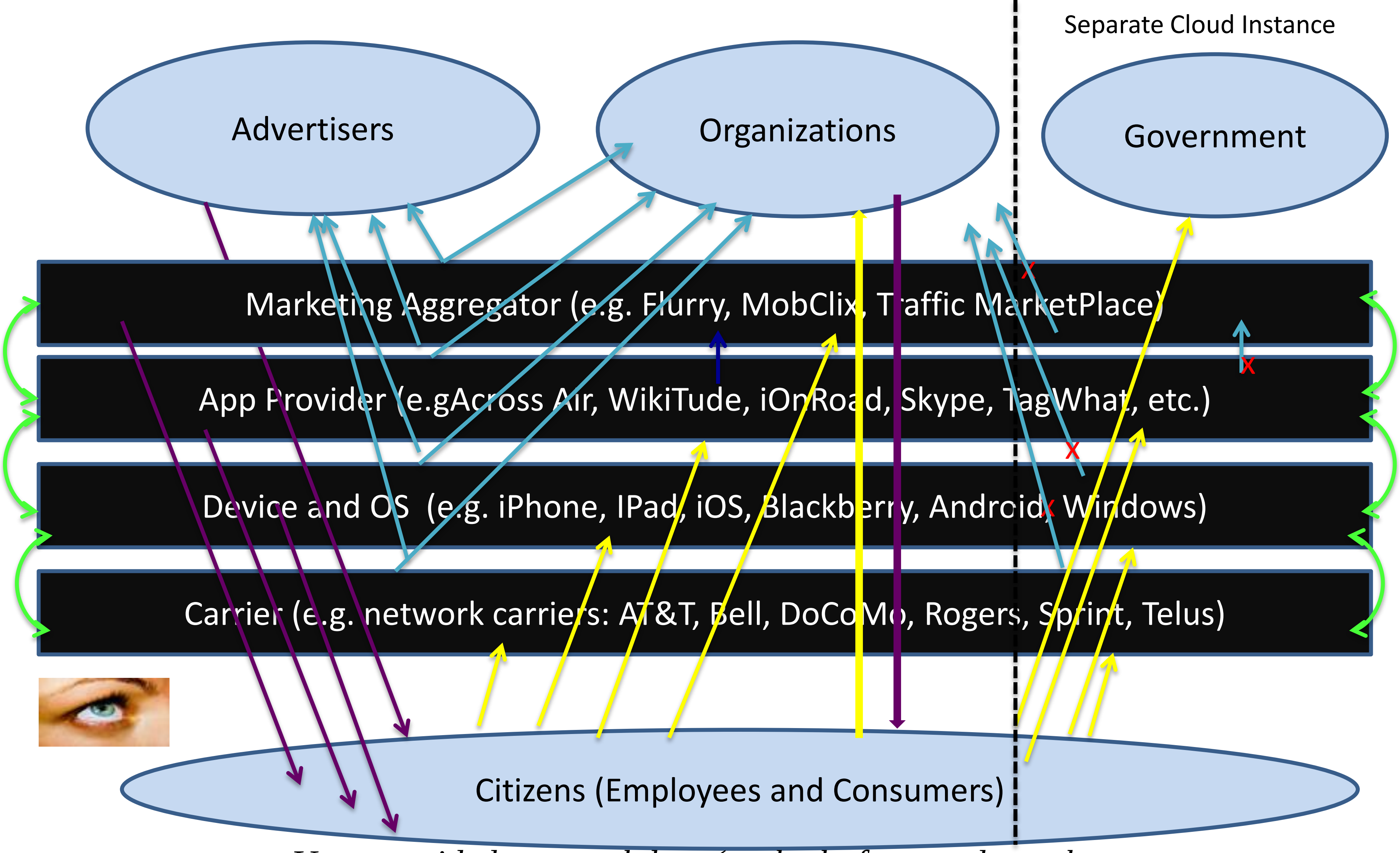

System
Review recommended treatments
Review Treatment
View alternative patients treatments
Analyze data
Doctor
Head Nurse
Data Scientist
Public Researcher



SSL – All communication over secure communication connection

PII Replacement – Replace PII with codes in program's input data

Privacy Notice – on storage and usage of obtained data
Agreement – Obtain agreement on storage and use of obtained data



Separate Cloud Instance

Advertisers

Organizations

Government

Marketing Aggregator (e.g. Flurry, MobClix, Traffic MarketPlace)

App Provider (e.gAcross Air, WikiTude, iOnRoad, Skype, TagWhat, etc.)

Device and OS (e.g. iPhone, IPad, iOS, Blackberry, Android, Windows)

Carrier (e.g. network carriers: AT&T, Bell, DoCoMo, Rogers, Sprint, Telus)

Citizens (Employees and Consumers)

User-provided personal data (each platform and merchant may get different data attributes) in a single service

User profiles sent to advertiser networks, aggregators, and to merchants

Ads, offers, deals etc.

Personal data flows between platforms.

Vision without Execution is Hallucination

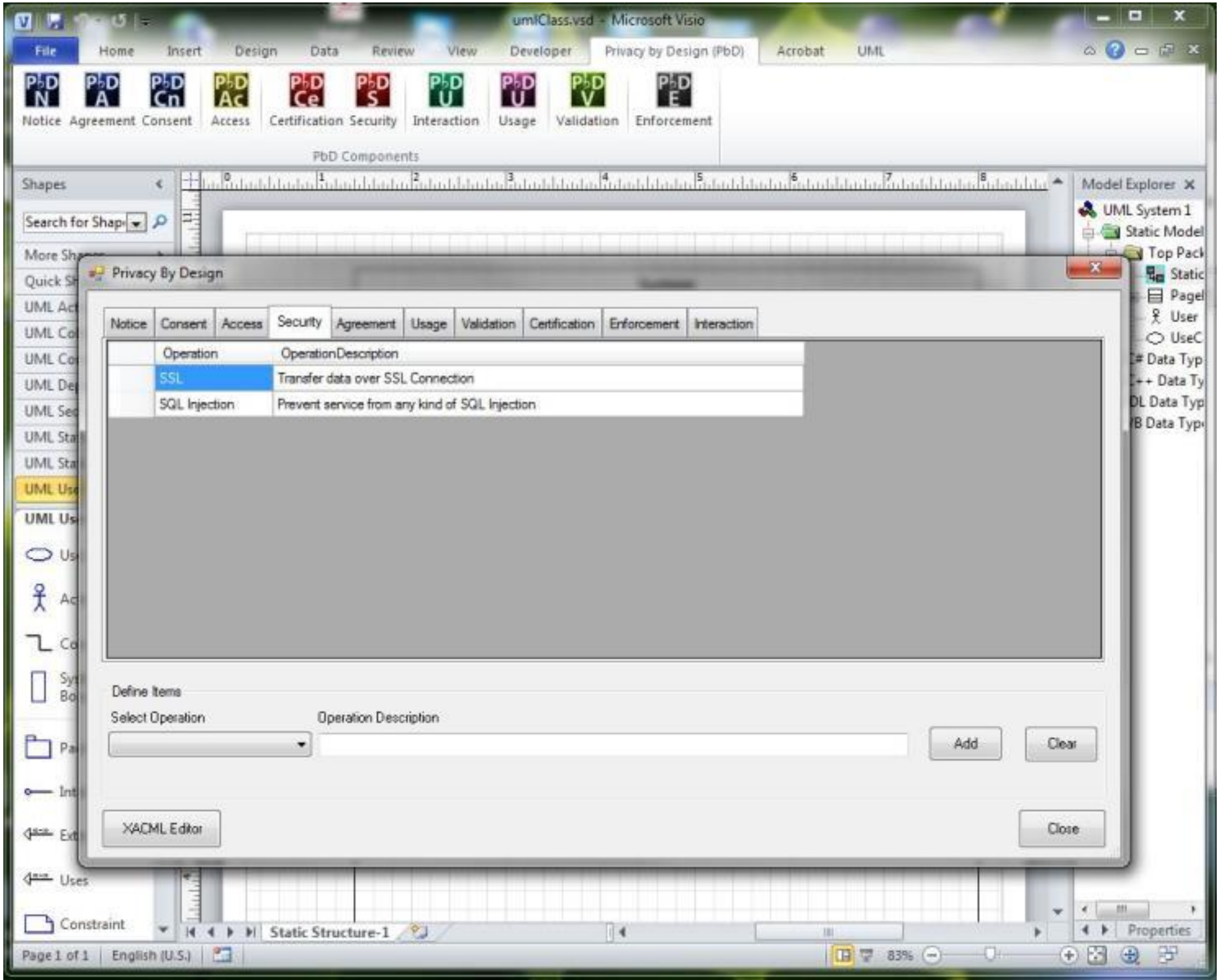
Examples of such documentation exist across industries but not CONSISTENTLY

Roles of Education and Adoption

Institutionalize Privacy Engineering within Software Engineering in Community College and University Programs
… in Computer Science, Engineering, Business, and the Arts

Create tools to make it EASIER for software engineers to comply to OASIS Emerging Privacy Standards without losing productivity

POSSIBLE FUTURE TOOLS IN SOFTWARE ENGINEERING EDUCATION/OASIS PbD-SE ADOPTION



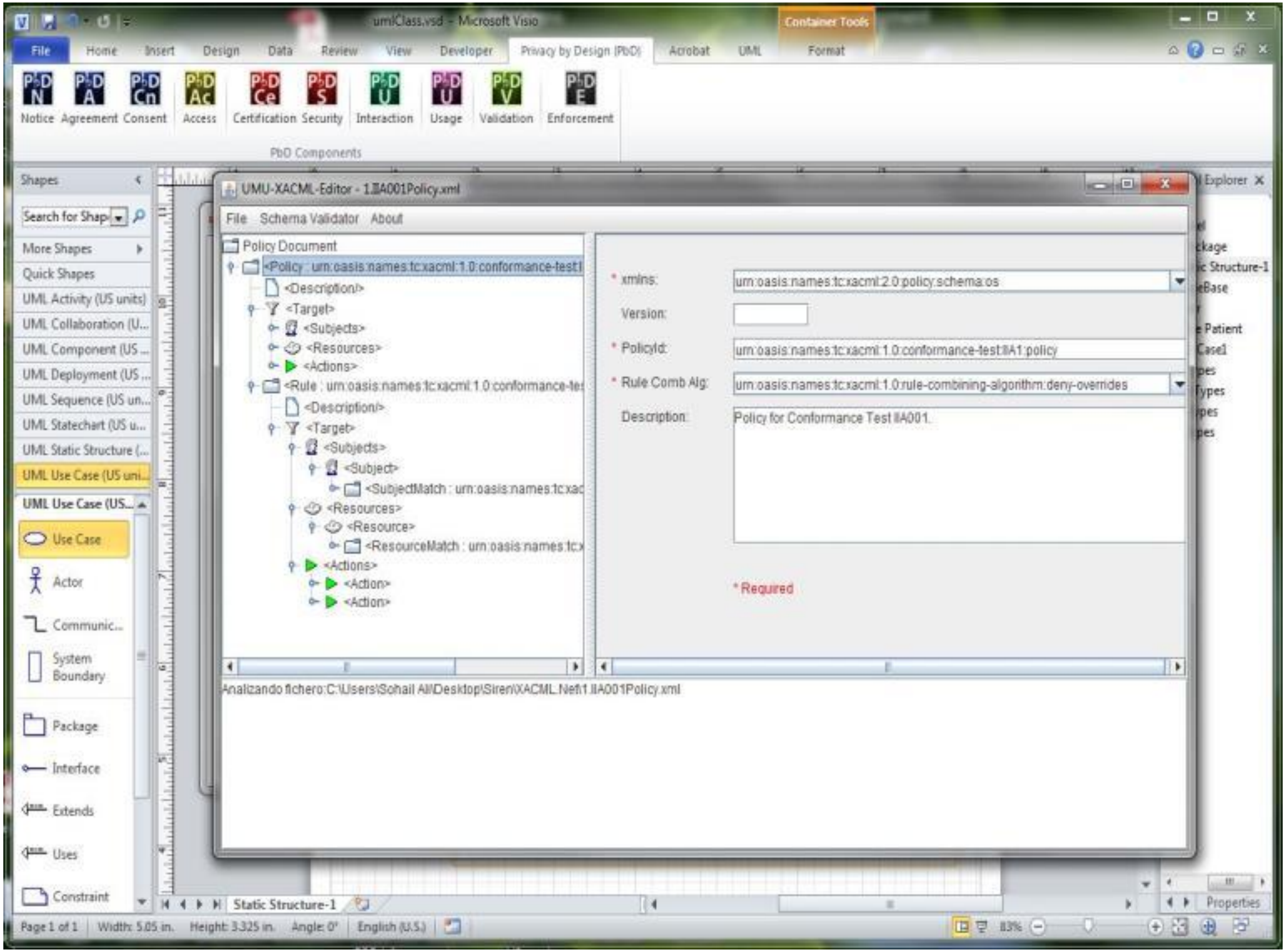
	Operation	OperationDescription
	SSL	Transfer data over SSL Connection
	SQL Injection	Prevent service from any kind of SQL Injection

Define Items

Select Operation

Operation Description

POSSIBLE FUTURE TOOLS IN SOFTWARE ENGINEERING – Example: UML tool with integrated XACML Editor



```
Policy Document
<Policy : urn:oasis:names:tc:xacml:1.0:conformance-test:I
    <Description/>
    <Target>
        <Subjects>
        <Resources>
        <Actions>
    <Rule : urn:oasis:names:tc:xacml:1.0:conformance-tes
        <Description/>
        <Target>
            <Subjects>
                <Subject>
                    <SubjectMatch : urn:oasis:names:tc:xac
            <Resources>
                <Resource>
                    <ResourceMatch : urn:oasis:names:tc:x
            <Actions>
                <Action>
                <Action>
```

* xmlns: urn:oasis:names:tc:xacml:2.0:policy:schema:os

Version:

* PolicyId: urn:oasis:names:tc:xacml:1.0:conformance-test:IIA1:policy

* Rule Comb Alg: urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides

Description: Policy for Conformance Test IIA001.

* Required

```
Analizando fichero:C:\Users\Sohail Ali\Desktop\Siren\XACML.Net\1.IIA001Policy.xml
```

STATUS CHECK ON THE PRIVACY FIELD

Status:	IMMATURE
Progress:	TOO SLOW
Funding:	UNDERFUNDED
Priority:	COMPETING INTERESTS – (all stakeholders)
Risk:	CITIZENS LOSE ALL PRIVACY
Impact:	IMMEASURABLE in terms of the freedoms of future generations

A lot more time-consuming work to do …

Our changing societies with wearables, wireless, augmented reality, big data, and IoT machines communicating (M2M).

©Julia Olmstead