Scalable Privacy, Trust & Confidence through evolving Open Standards

8th ETSI Security Workshop
16-17 January 2013
Sophia Antipolis

Gershon Janssen  @gershonjanssen
Use Case: Electric Cars

Benefits:
• Cost savings
• Environmental
Downside:
• Limited range
• Charging
Developments

- Roll-out of charge points
- More car models
- Attractive financial arrangements:
  - Lower or no taxes
  - No parking fees
- More possibilities:
  - Easy settlement and billing
  - Insights on usage
EV eco-system starts to emerge...
EV eco-system expands...

Source: Siemens AG
...new challenges play up!

**Security**
- Access Control, Credential Management

**Privacy**
- Customer ID, Location Data, Vehicle ID

**Deployment**
- Cloud Deployment, Portability, Multi-Cloud

**Identity**
- Federated Identity, Trust Levels

Source: Siemens AG
Open Standards as Building Blocks

• Privacy
  • PMRM – Privacy Management Reference Model
  • PdB-SE – Privacy By Design for Software Engineers

• Security:
  • XACML – eXtensible Access Control Markup Language
  • KMIP – Key Management Interoperability Protocol

• Identity Management and Trust
  • IDCloud – Identity in the Cloud
  • Trust-El – Electronic Identity Credential Trust Elevation Methods

• Cloud
  • TOSCA – Topology and Orchestration Specification for Cloud Applications
Privacy Management Reference Model and Methodology

- **What is it?**
  - It is a tool that helps improve privacy management and compliance in complex environments where the use of personal information (PI) is governed by laws, regulations, business contracts and other policies.

- **What to use it for?**
  - To analyze complex use cases.
  - To understand and implement appropriate operational privacy management functionality and mechanisms.
  - To achieve compliance across policy, system and ownership boundaries.
  - To design a privacy management architecture for operational environments.
The model provides a common conceptual framework and vocabulary to help people cooperate across disciplines and organizational boundaries...

...and the methodology provides a common set of tasks to achieve a privacy architecture and privacy management analysis.
The PMRM Model

Privacy Controls

PMRM Services

Technology

Laws & Regulations

Privacy Domain

Privacy Architecture

Policies & Principles

Stakeholders

Use Cases

Core Concerns (protection of PI/PII)

OASIS
The PMRM Methodology

1. Define the Scope of the Use Case
   - Description and inventory of services/applications
   - Privacy requirements (including FIPPs)
   - Impact/Other Assessments

2. Conduct Detailed Use Case Analysis
   - Actors and Systems
   - Domains and Owners
   - Roles and Responsibilities
   - Data Flows and Touch Points
   - Incoming, Internally Generated and Outgoing PI for all actors and systems

3. Specify Operational Privacy Control Requirements
   - Inherited
   - Internal
   - Exported

4. Associate PMRM Services
   - Agreement
   - Usage
   - Validation
   - Certification
   - Enforcement
   - Security
   - Interaction
   - Access


6. Perform Risk/Compliance Assessment

Create Privacy Management Analysis

Develop Privacy Architecture

Implementation
High-Level Privacy Analysis and Use Case

**Inputs:**
Privacy Impact Assessments
Privacy Maturity Assessments
Compliance Reviews
Accountability Model Assessments
Detailed Privacy Use Case Analysis

Identify all the following:

- Domains
- Touch Points
- Systems
- Roles & Responsibilities
- Owners
- Actors
Identify PI collected, created, communicated, processed or stored and Privacy Controls
Services Supporting Privacy Controls

Privacy Controls are usually stated in the form of a policy declaration or requirement and not in a way that is immediately actionable or implementable.

Services provide the ‘bridge’ between requirement and implementation by providing privacy constraints on system-level actions governing the flow of PI between touch points.

8 key PMRM Services identified in the initial work:

- Agreement
- Validation
- Certification
- Interaction
- Usage
- Security
- Enforcement
- Access
Services Supporting Privacy Controls

- Services are sets of related functions to support the identification of the specific operational mechanisms to implement Privacy Controls.

- An systems architect should be able to implement any set of privacy policies by integrating the Services into a functional architecture and subsequently select mechanisms to implement the specific functions.
Map Privacy Controls to Services

Incoming PI

Inherited Privacy Controls

PMRM Services Required

Internally Generated PI

Internal Privacy Controls

Outgoing PI

Exported Privacy Controls
Map Services to Functions

PMRM Services Used

<table>
<thead>
<tr>
<th>Ag</th>
<th>E</th>
<th>Ac</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>V</td>
<td>S</td>
</tr>
<tr>
<td>U</td>
<td>V</td>
<td>E</td>
</tr>
<tr>
<td>U</td>
<td>V</td>
<td>S</td>
</tr>
</tbody>
</table>

Business Processes and Technical Mechanisms Required

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>C</td>
<td>E</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>C</td>
<td>D</td>
<td>G</td>
<td>H</td>
</tr>
<tr>
<td>C</td>
<td>E</td>
<td>G</td>
<td>H</td>
<td></td>
</tr>
</tbody>
</table>
Privacy by Design for Software Engineers

What is it?

- Provides privacy governance and documentation standards for software engineers.
- Enables software organizations to embed privacy into the design and architecture of IT systems, without diminishing system functionality.
- PbD-SE follows the Seven Foundational Principles of Privacy by Design.
- PbD-SE offers a privacy extension/complement to OMG’s Unified Modeling Language (UML) and serves as a complement to OASIS’ eXtensible Access Control Mark-up Language (XACML) and Privacy Management Reference Model (PMRM).
Privacy by Design for Software Engineers

The Seven Foundational Principles of Privacy by Design:

1. Proactive not Reactive; Preventative Not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality - Positive-Sum, Not Zero-Sum
5. End-to-End Security - Full Lifecycle Protection
6. Visibility and Transparency - Keep It Open
7. Respect for User Privacy - Keep It User-Centric
Identity & Trust

- **IDCloud – Identity in the Cloud**
  - Identified use cases for Cloud Identity Management
  - Gap analyses on existing Identity Management standards
  - Provides Interoperability Profiles
  - Glossary on Cloud Identity

- **Trust-El – Electronic Identity Credential Trust Elevation Methods**
  - Elevate the trust in an electronic identity presented for authentication purposes.
  - Transaction-based assurance: “authentication” based on the necessary current conditions
  - Defines a set of methods and / or standardized protocols to elevate the trust in an electronic identity.
Cloud Deployment

- **TOSCA – Topology and Orchestration Specification for Cloud Applications**
  - Allows for the interoperable description of application and infrastructure cloud services, the relationships between parts of the service, and the operational behavior of these services (e.g., deploy, patch, shutdown)—independent of the supplier creating the service, and any particular cloud provider or hosting technology.
  - Enables:
    - Portable deployment to any compliant cloud
    - Smoother migration of existing applications to the cloud
    - Flexible bursting (consumer choice)
    - Dynamic, multi-cloud provider applications
Links and References

- **OASIS Technical Committee Homepages**
  - [http://www.oasis-open.org/committees/pmrm](http://www.oasis-open.org/committees/pmrm)
  - [http://www.oasis-open.org/committees/pbd-se](http://www.oasis-open.org/committees/pbd-se)
  - [http://www.oasis-open.org/committees/idcloud](http://www.oasis-open.org/committees/idcloud)
  - [http://www.oasis-open.org/committees/trust-el](http://www.oasis-open.org/committees/trust-el)
  - [http://www.oasis-open.org/committees/tosca](http://www.oasis-open.org/committees/tosca)

- **Gershon Janssen**
  - gershon.janssen@gmail.com
  - @gershonjanssen