On the Need to Explicitly Manage Privacy Obligation Policies as Part of Good Data Handling Practices

Marco Casassa Mont

marco.casassa-mont@hp.com

Hewlett-Packard Labs

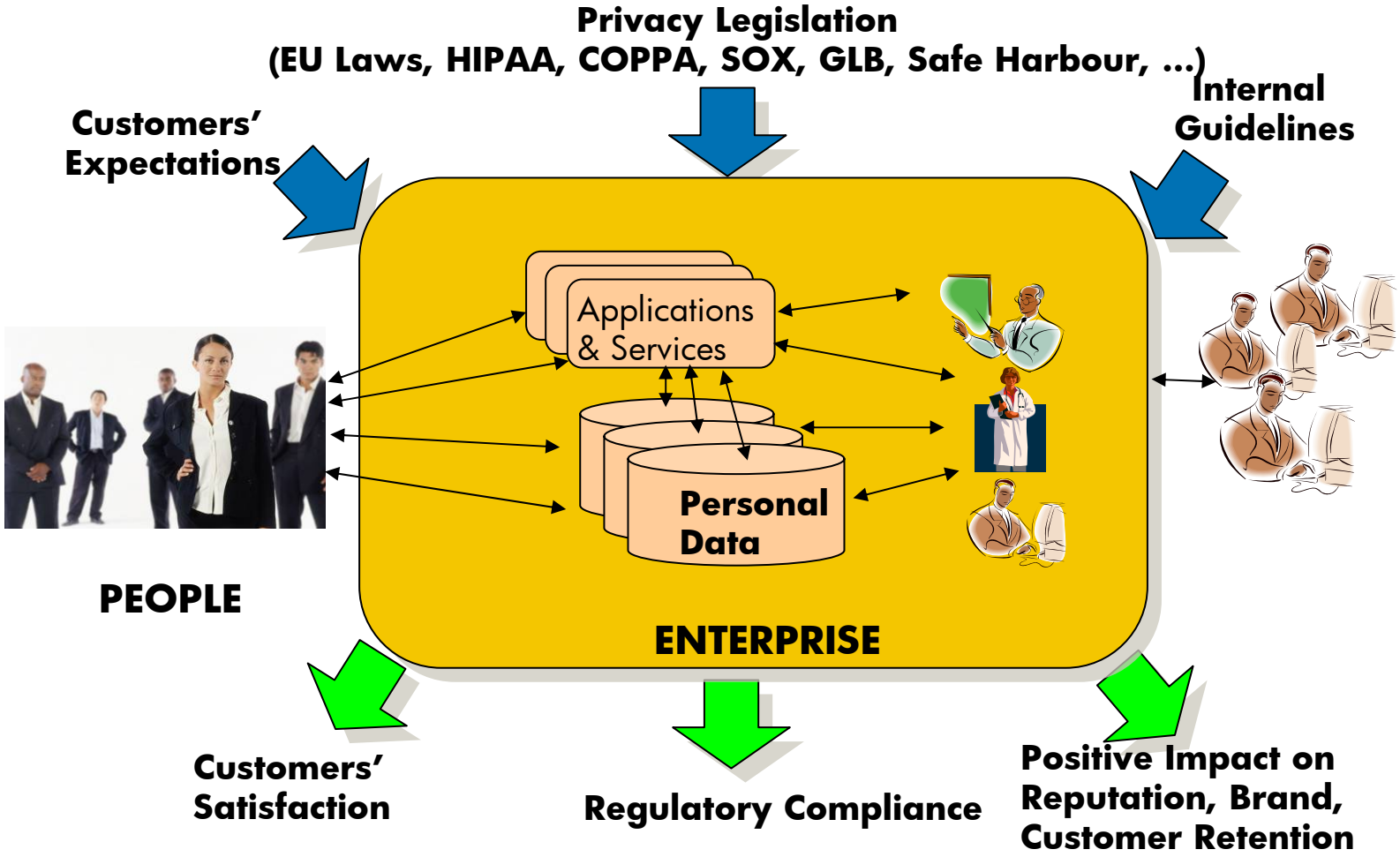
Presentation Outline

- Privacy Concepts and Background
- Our Position
- Privacy Obligations
- Current Work, Limitations & Suggested Approach
- Requirements
- An Example: Work Done in PRIME
- Proposed Next Steps

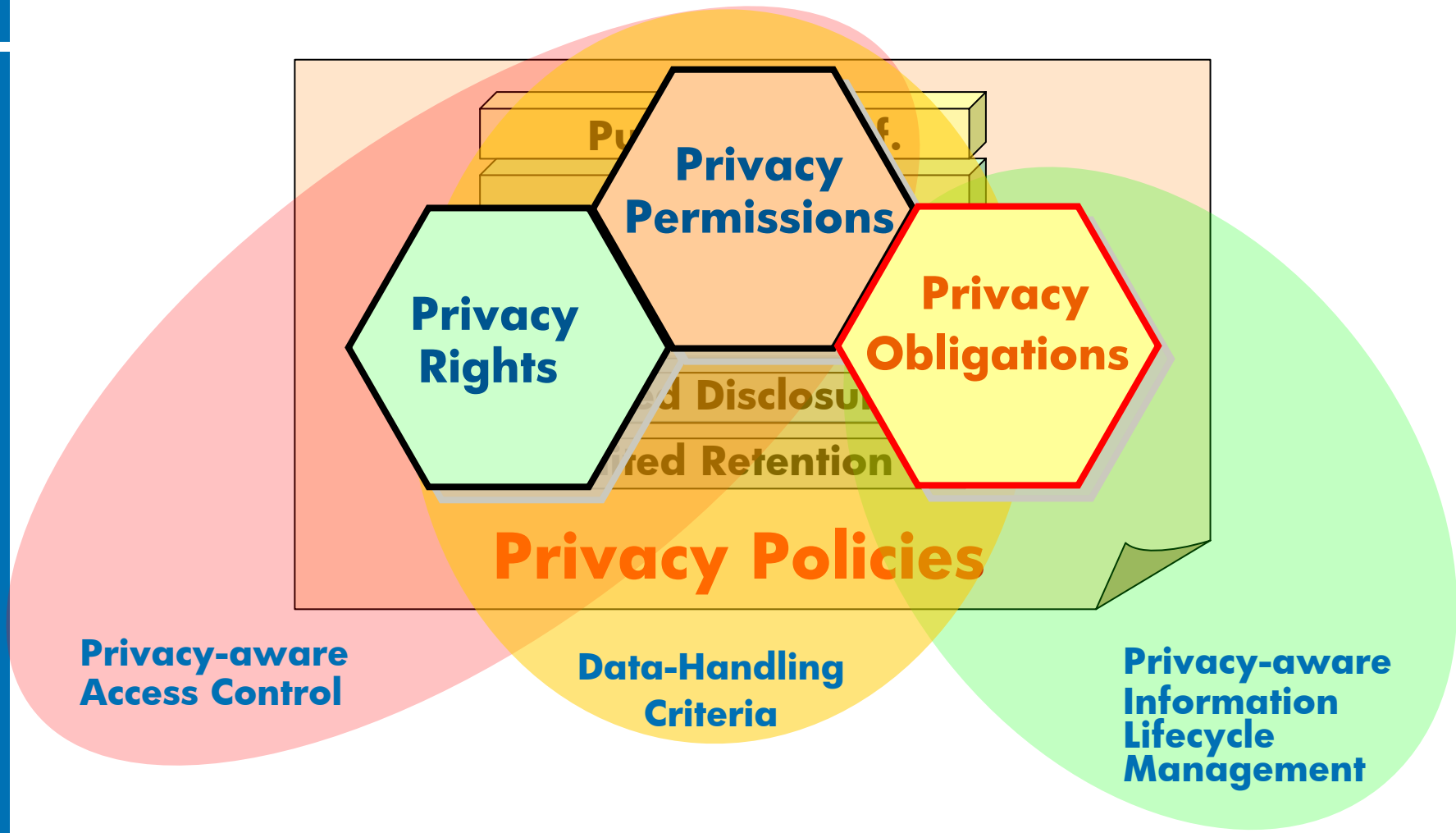
Presentation Outline

- Privacy Concepts and Background
- Our Position
- Privacy Obligations
- Current Work, Limitations & Suggested Approach
- Requirements
- An Example: Work Done in PRIME
- Proposed Next Steps

Privacy: Impact on Users and Enterprises



Privacy Policies & Data Handling on PII Data



Presentation Outline

- Privacy Concepts and Background
- Our Position
- Privacy Obligations
- Current Work, Limitations & Suggested Approach
- Requirements
- An Example: Work Done in PRIME
- Proposed Next Steps

Our Position

- Need to Recognise Complementary Roles of Obligation Policies and Access Control Policies
- No Subordination of Obligations to Access Control Policies: share Data Handling Criteria
- Need to Explicitly Represent, Manage and Enforce Obligations
- Opportunity in defining "Integrated Language" covering both Access Control and Obligation Aspects and Multiple, Specialised Policy Enforcement Solutions
- Go for Standardisation for Interoperability/Negotiation
- Keep into account Current Identity Management Solutions …

Presentation Outline

- Privacy Concepts and Background
- Our Position
- Privacy Obligations
- Current Work, Limitations & Suggested Approach
- Requirements
- An Example: Work Done in PRIME
- Proposed Next Steps

Privacy Obligations

- Privacy Obligations are Policies that describe Duties and Expectations on how PII Data Should be Managed, in particular by Enterprises (e.g. Deletion, Notifications, Data Transformation ,etc.)
- They are at the very base of "Privacy-aware Information Lifecycle Management"
- They can be dictated by Law, Data Subjects' Preferences and Enterprise Guidelines

Privacy Obligations: Abstract vs. Refined

Obligations can be very Abstract:

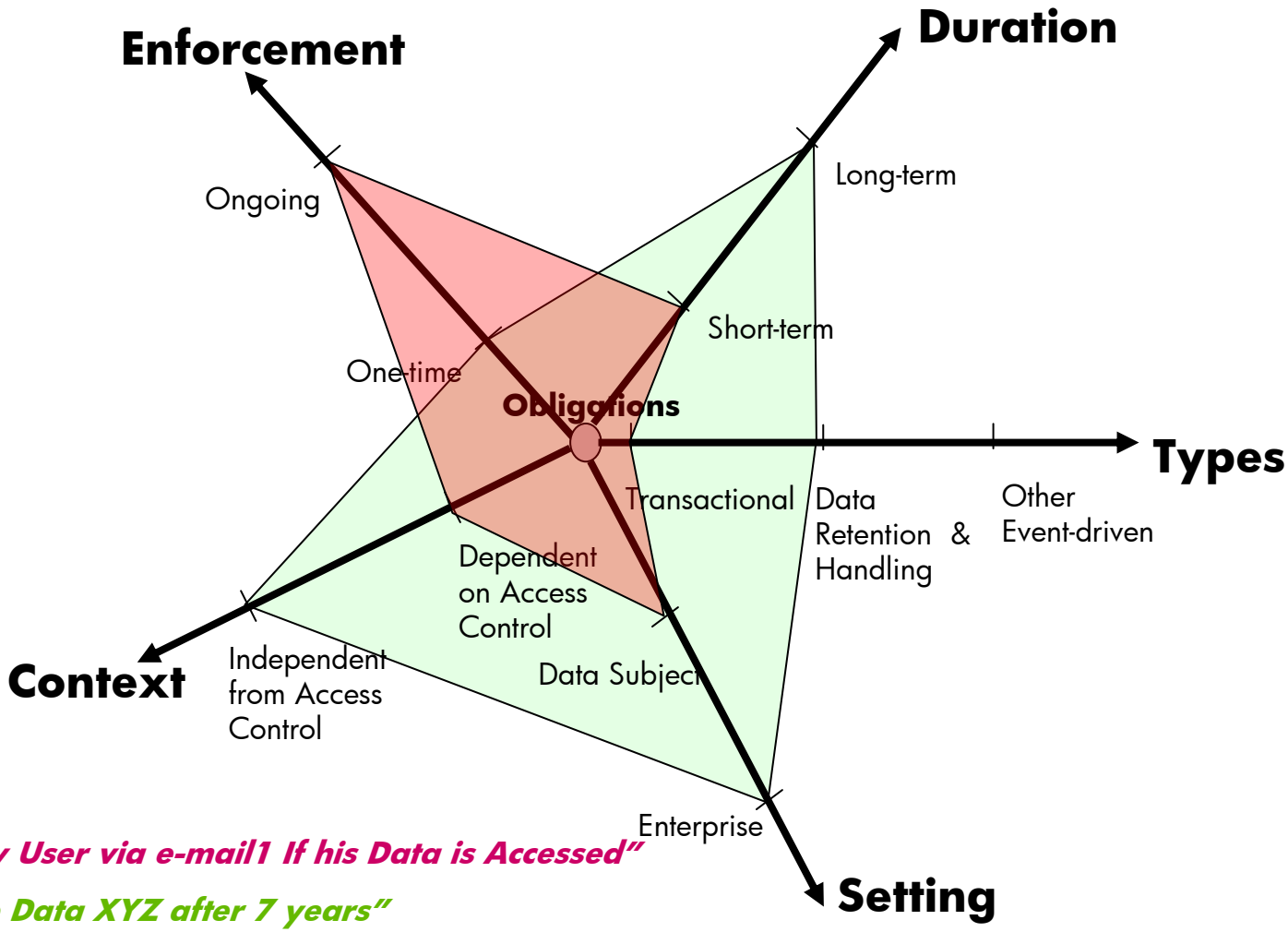
"Every financial institution has an affirmative and continuing obligation to respect customer privacy and protect the security and confidentiality of customer information"

Gramm-Leach-Bliley Act

More Refined Privacy Obligations dictate Duties and Responsibilities with respect of Personal Information:

- **Notice Requirements**
- **Enforcement of opt-in/opt-out options**
- **Limits on reuse of Information and Information Sharing**
- **Data Retention limitations …**

Privacy Obligations: A Complex Topic …

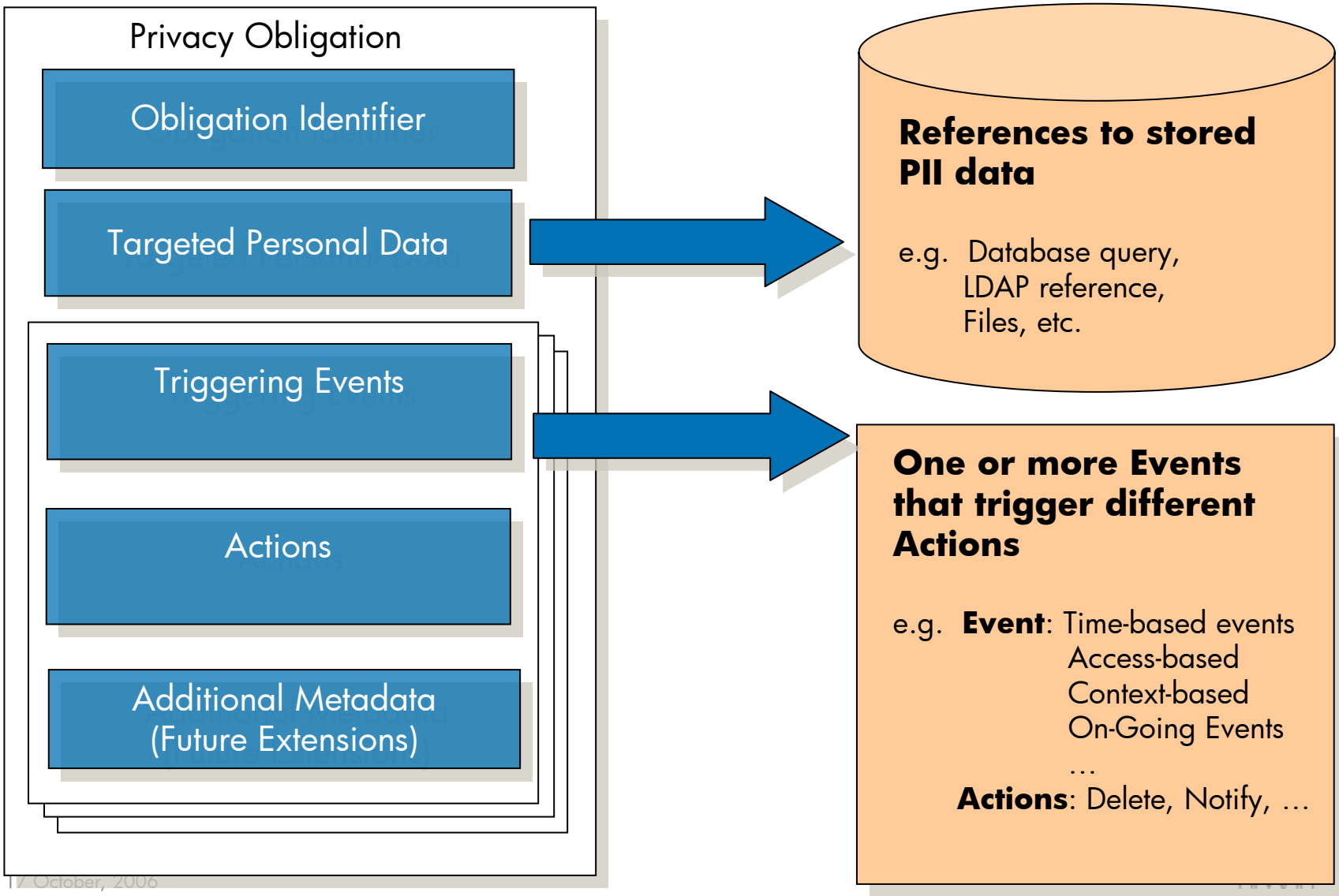


"How Represent Privacy Obligations? How to Stick them to Personal Data?
How to Manage, Enforce and Monitor them? How to Integrate them into current IDM solutions?"

Privacy Obligations: Key Properties

- **Timeframe** (period of validity) of obligations
- **Events/Conditions** that trigger the need to fulfil obligations
- **Target** of an obligation (PII data)
- **Actions/Tasks/Workflows** to be Enforced
- **Responsible** for enforcing obligations
- **Exceptions** and special cases

Privacy Obligation: Conceptual Model



Presentation Outline

- Privacy Concepts and Background
- Our Position
- Privacy Obligations
- Current Work, Limitations & Suggested Approach
- Requirements
- An Example: Work Done in PRIME
- Proposed Next Steps

Related Work [1/2]

- P3P (W3C):
  - Definition of User's Privacy Expectations
  - Explicit Declaration of Enterprise Promises
  - No Framework/definition of Mechanisms for their Enforcement
- Data Retention Solutions and Document Management Systems.
  - Limited in terms of expressiveness and functionalities.
  - Focusing more on documents/files, not really on personal data
- Ad-hoc Solutions for Vertical Markets

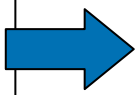
Related Work [2/2]

Recent relevant Work done in this Space:

- IBM Enterprise Privacy Architecture, including a policy management system, a privacy enforcement system and audit

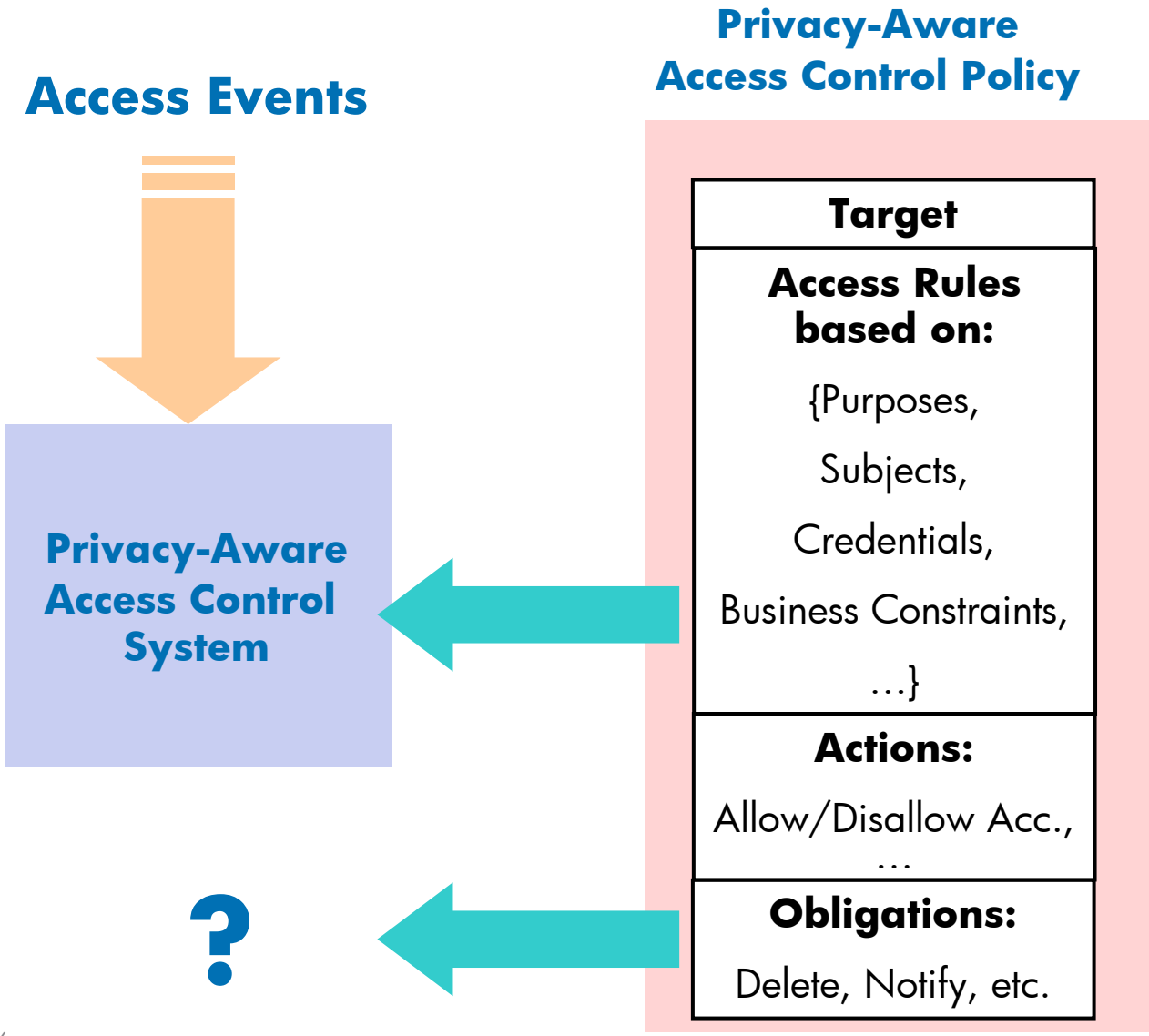
- Initial work on privacy obligations in the context of Enterprise Privacy Authorization Language (EPAL)

- XACML (OASIS): Access Control-focused standard

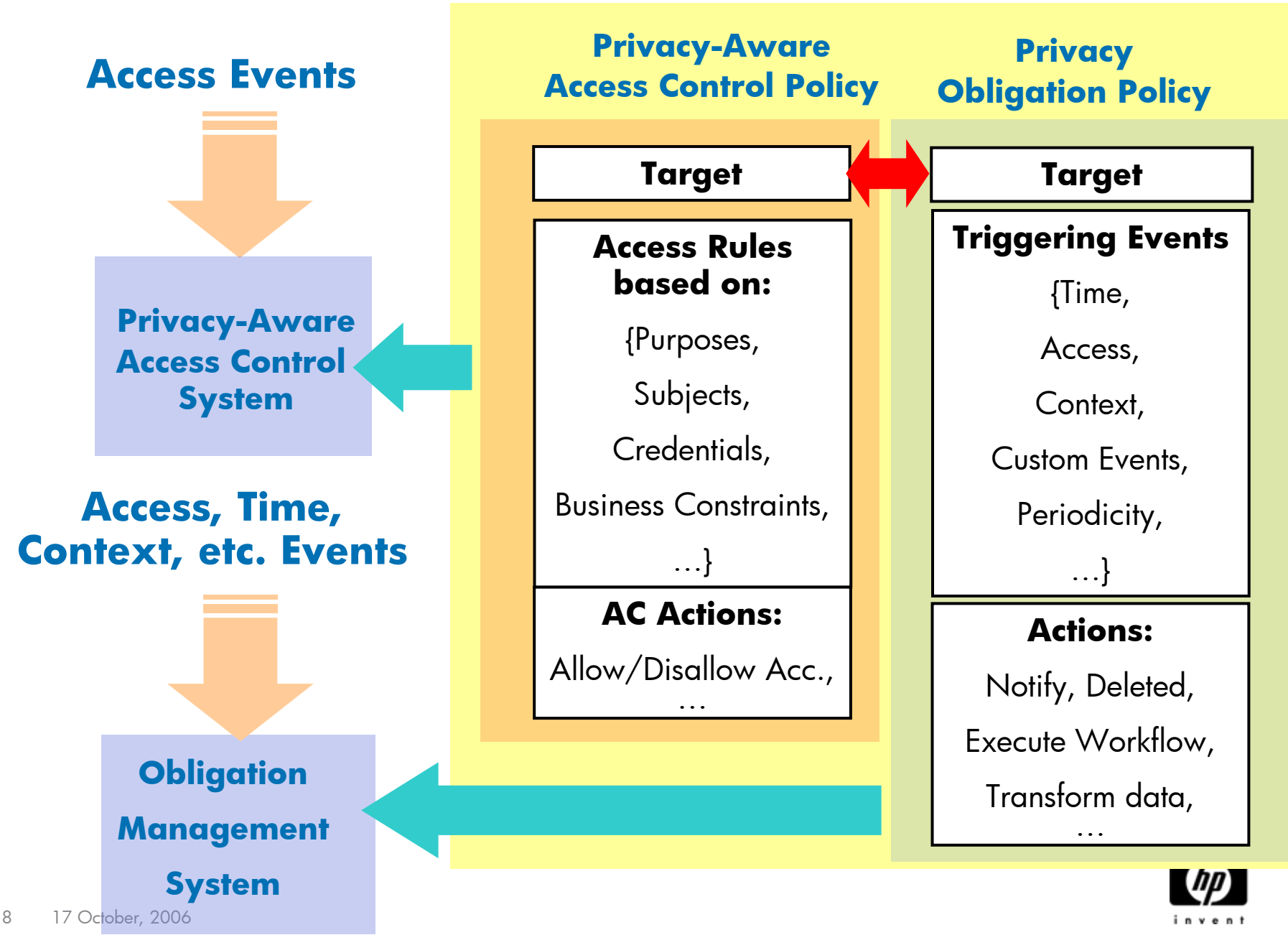


- No Refined Model of Privacy Obligations
- Privacy Obligations Subordinated to AC …

"Access Control – Centric" Approach (XACML, EPAL, …)



More "Suitable" Approach …



Presentation Outline

- Privacy Concepts and Background
- Our Position
- Privacy Obligations
- Current Work, Limitations & Suggested Approach
- Requirements
- An Example: Work Done in PRIME
- Proposed Next Steps

Requirements [1/2]

- Need for a "Language" to Explicitly Represent Privacy Obligations (Target, Events, Actions, …)
- Integration with Privacy-aware Access Control Language →No Subordination …
- Being able to use suitable Ontologies whose Semantic is shared with Access Control Constraints
- Common Data Handling Criteria shared by Access Control and Obligation Policies
- Possibly Leverage/Extend/Modify Current Standards (XACML, etc.) or Ensure Compatibility/Interoperability → Importance of Standardisation!

Requirements [2/2]

- Explicit Association of Obligations to PII Data
- Need to Define Enforcement Framework for Obligations (Scheduling, Enforcement, Monitoring)
  → No Subordination to Access Control
- Ensure Compatibility with State-of-Art Identity Management Solutions
- Need to Deal with Negotiation of Data Handling Criteria and Obligations
  → Do First Steps First i.e. Language & Enforcement Framework

Presentation Outline

- Privacy Concepts and Background
- Our Position
- Privacy Obligations
- Current Work, Limitations & Suggested Approach
- Requirements
- An Example: Work Done in PRIME
- Proposed Next Steps

EU PRIME Project: Obligation Management

Enabling Privacy-aware Information Lifecycle Management:

Data Subjects

Privacy Preferences

Obligations Monitoring

Obligations Scheduling

Obligations Enforcement

Obligation Management Framework

Administrators

Privacy Obligations

Personal Data (PII)

ENTERPRISE

Privacy Obligations: Operational View

Obligations As "Reactive Rules"

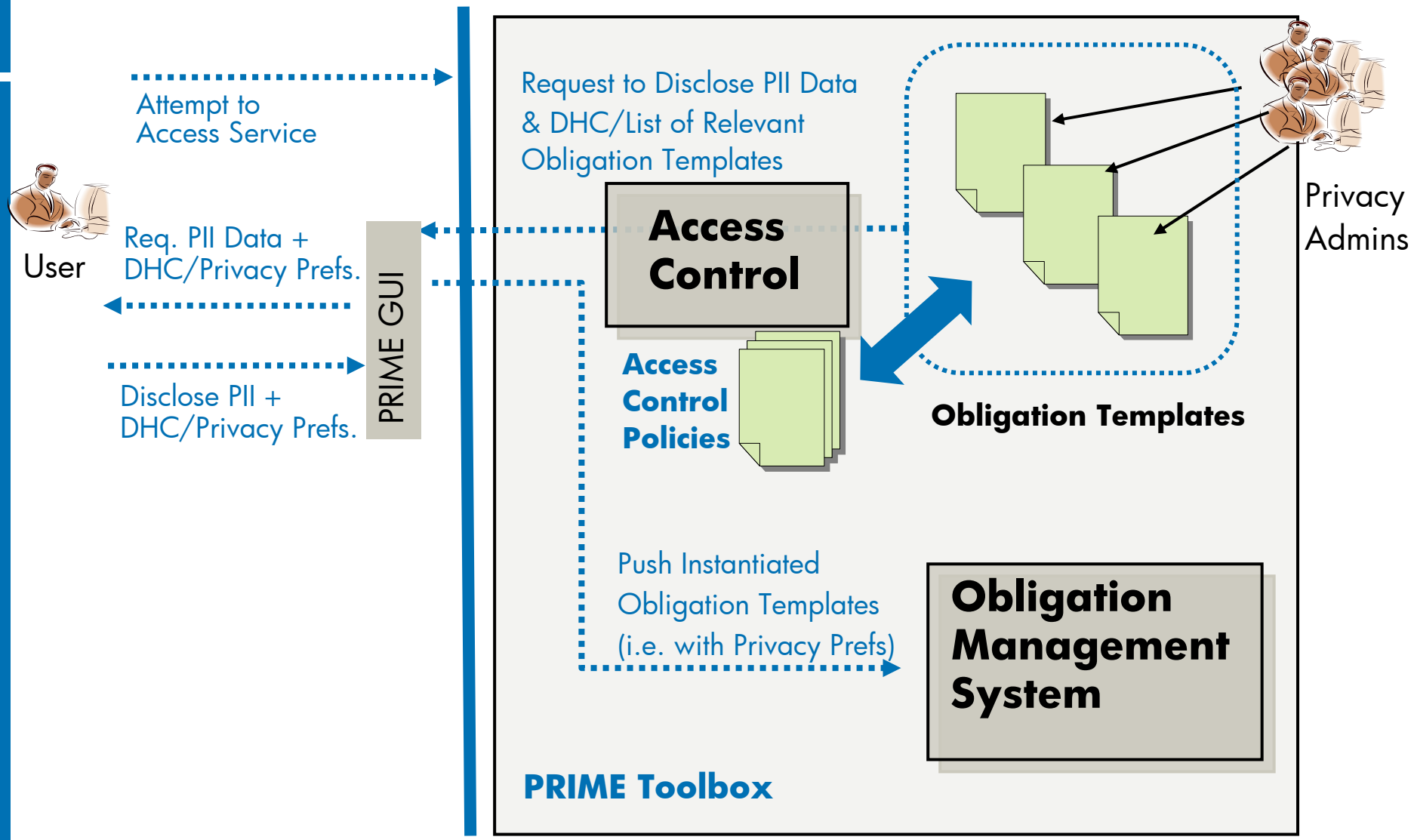
OBLIGATION Oid:

TARGETS: TargetRefs

WHEN LogicalCombinationOf (EVENTS)

EXECUTE CompositionOf (ACTIONS)

EU PRIME Project: (Loosely) Integrated Approach



Obligation Template:
- Defines Obligation Structure
- Defines Types of Privacy Prefs

ENTERPRISE

EU PRIME Project: Key Open Issues

- Loose Integration of AC Policies with Obligation Policies
  → Need for Common Language

- Obligations Share Data Handling Criteria (DHC). OK!

  →Need to Standardise these Data Handling Criteria for:
  - Interoperability
  - Enabling Negotiation (Client/Enterprise, Multi-Party)

- No Negotiation of Complex DHC …

Presentation Outline

- Privacy Concepts and Background
- Our Position
- Privacy Obligations
- Current Work, Limitations & Suggested Approach
- Requirements
- An Example: Work Done in PRIME
- Proposed Next Steps

Proposed Next Steps

- Consider work Done in PRIME …
- Collect Requirements. Gain support from Industry
- Explore Alternative Approaches to Obligation Management, if required …
- Analyse and Design Integrated Language to Explicitly Describe both AC Rules and Obligations – Common DHP
- Standardise this Language and Ensure it can be used by a suitable Enforcement/Management Framework
- Ensure Compatibility with current Identity Management Initiatives
- Address Aspects such as Sticky Policies and Negotiation …

BACK-UP SLIDES

Open Issues and Next Steps

- Current Approach

  Pros

  - Flexible Language and Approach
  - Extensible and Customisable

  Cons

  - Large Set of Similar Obligations might be Created
  - Scalability Issues

- Next Steps
  - Address Scalability Issues
  - Introduce Parametric Obligations
  - Extend Language (Exceptions, more types of Events, Actions, etc.)

Privacy Obligations: Formal View

Privacy Obligation is a *<i,t,L(e),C(a)>* tuple

$$\langle i,t,e,a \rangle \in \langle I, 2^T, 2^E, 2^A \rangle$$

$i \in I$: set of all unique identifiers

$t \subseteq T$: set of all possible targets

$e \subseteq E$: set of all possible events

$a \subseteq A$: set of all possible actions

- ***L(e)*** **: defines a logical combination (AND, OR, NOT) of events**
- ***C(a)*** **: defines an operational combination of actions, such as a sequence of actions**

Privacy Obligation Examples

Delete PII Data at a Predefined Time

1) *OBLIGATION Oid1:*

TARGETS:

t1:< DATABASE=db1, TABLE=customers, Key=CustomerName, KeyValue=abc>

WHEN (current_time= date1)

EXECUTE <DELETE t1>

Notify Users when their PII Data is Accessed

2) *OBLIGATION Oid2:*

TARGETS:

t1:< DATABASE=db1, TABLE=customers, Key=CustomerName, KeyValue=abc,

ATTRIBUTES=(e-mail) >

WHEN (Access_Data_Event AND Access_Data_Event.data = t1)

EXECUTE <NOTIFY BY t1.e-mail>

Privacy Obligation Examples

Notify Users and Delete PII Data when it is not Accessed after a Predefined Date

3) ***OBLIGATION Oid3:***

TARGETS:

t1:< DATABASE=db1, TABLE=customers, Key=CustomerName, KeyValue=abc ATTRIBUTES=(creditcard,e-mail)>

WHEN

(current_time>date1)

AND

(NOT (Access_Data_Event AND Access_Data_Event.data = t1))

EXECUTE

<NOTIFY BY t1.e-mail>

<DELETE t1.creditcard>

Privacy Obligation Examples

Delete PII Data and De-provision a User Account either after a specified Date Or if PII Data has been Accessed more than n Times

4) ***OBLIGATION Oid4:***

TARGETS:

t1:< DATABASE=db1, TABLE=customers, Key=CustomerName, KeyValue=abc

ATTRIBUTES=(creditcard,e-mail)>

WHEN

(current_time>date1)

OR

((Access_Data_Event AND Access_Data_Event.data = t1)

AND

(Access_Counter>n))

EXECUTE

<DELETE t1.creditcard>

<RUN WORKFLOW deprovision_user(t1.KeyValue)>

Privacy Obligation Examples

Notify Users on Ongoing Bases at a Specified Interval of Time

5) ***OBLIGATION Oid5:***

TARGETS:

t1:< DATABASE=db1, TABLE=customers, Key=CustomerName, KeyValue=abc,
ATTRIBUTES=(e-mail)>

WHEN

(current_time < date1)
AND
(time_counter > time_interval)

EXECUTE

<NOTIFY BY t1.email>
<RESET time_counter>

Privacy Obligation Examples

Encrypt PII Data and Notify the administrator in case of Intrusion

6) *OBLIGATION Oid6:*
TARGETS:
t1:< DATABASE=db1, TABLE=customers>
WHEN
(Event-intrusion_detected)
EXECUTE
<ENCRYPT t1>
<NOTIFY admin>

Encrypt PII Data and Notify the administrator in case the System is in an inconsistent/Distrusted state

7) *OBLIGATION Oid7:*
TARGETS:
t1:< DATABASE=db1, TABLE=customers>
WHEN
(Event-system_distrusted)
AND
(DATABASE.host =system_distrusted.host)
EXECUTE
<ENCRYPT t1>
<NOTIFY admin>

Privacy Obligation Examples

Encrypt Address Attributes and Delete User Names in Log Files older than 6 months

8) ***OBLIGATION Oid8:***

TARGETS:

t1:< FILE=../audit_log, ATTRIBUTES=(TimeStamp, UserIPaddress, UserName)>

WHEN

(time_counter > time_interval)

EXECUTE

<ENCRYPT t1.UserIpAddress>

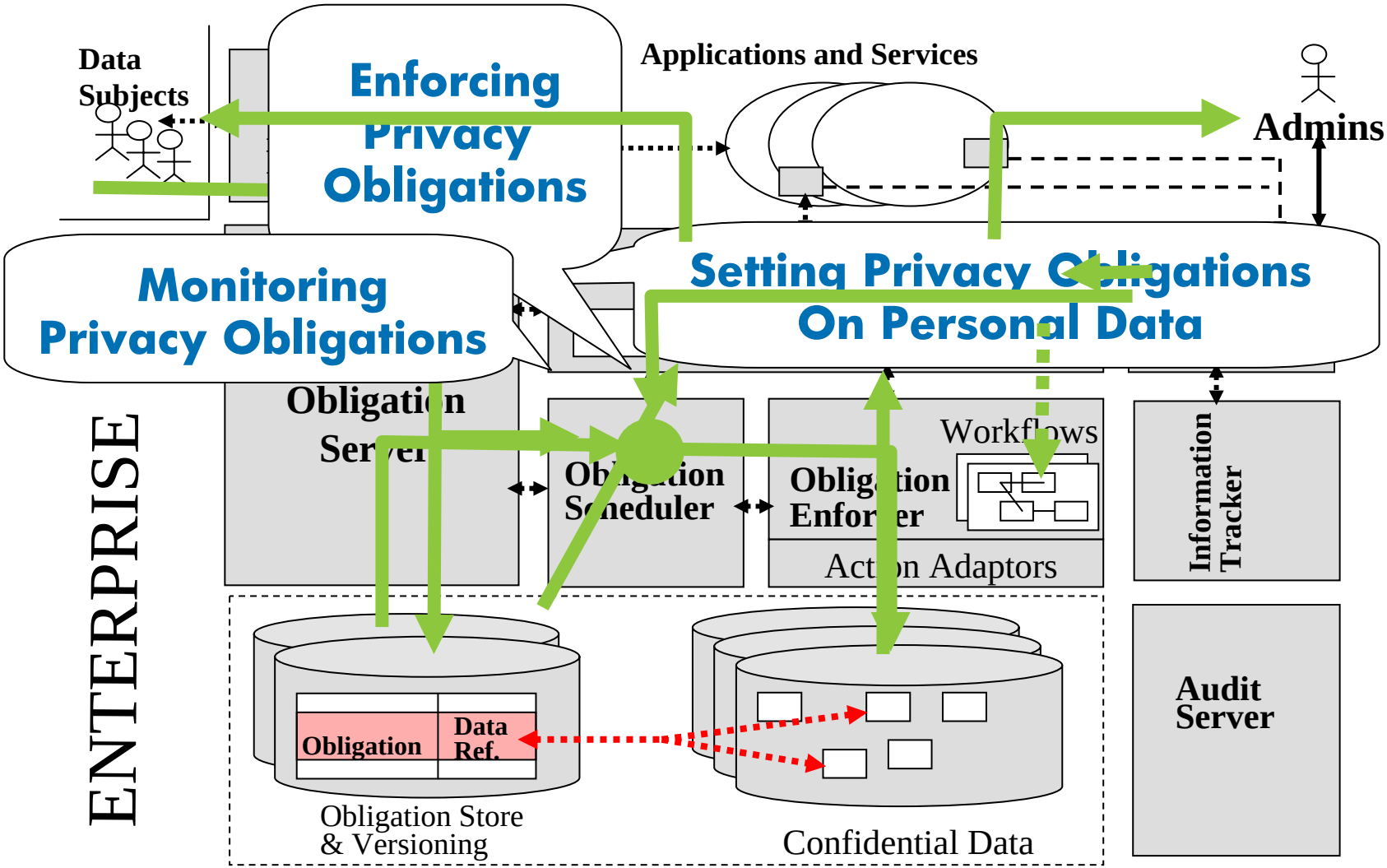
<DELETE t1.UserName WHERE t1.TimeStamp<= current_time - 6 months>

<RESET time_counter>

Privacy Obligations: PRIME Representation in XML Format

```
<obligation id="gfrbg7645gt45">
    <target>
        <database>
            <dbname>CustomersDB</dbname>
            <tname>Customers</tname>
            <locator>
                <key name="UserID">oid_a83b8a:fdfc44df3b:-7f9c</key>
            </locator>
            <data attr="part"> <item>creditcard</item> <item>firstname</item> </data>
        </database>
    </target>
    <obligationitem sid="1">
        <metadata>
            <type>LONGTERM</type>
            <description>Delete [creditcard,firstname] at Aug 15 17:26:21 BST 2006.]</description>
        </metadata>
        <events>
            <event>
                <type>TIMEOUT</type>
                <date now="no">
                    <year>2006</year> <month>08</month>
                    <day>15</day> <hour>17</hour><minute>26</minute>
                </event>
        </events>
        <actions>
            <action>
                <type>DELETE</type>
                <data attr="part"> <item>creditcard</item> <item>firstname</item> </data>
            </action>
        </actions>
    </obligationitem>
</obligation>
```

Obligation Management System (OMS): High Level System Architecture




invent