

EPAL Enterprise Privacy Authorization Language

Privacy Policies for Enterprise-internal Use

Michael Waidner, IBM Research, Zurich, acting for:

Paul Ashley, IBM Tivoli, Australia

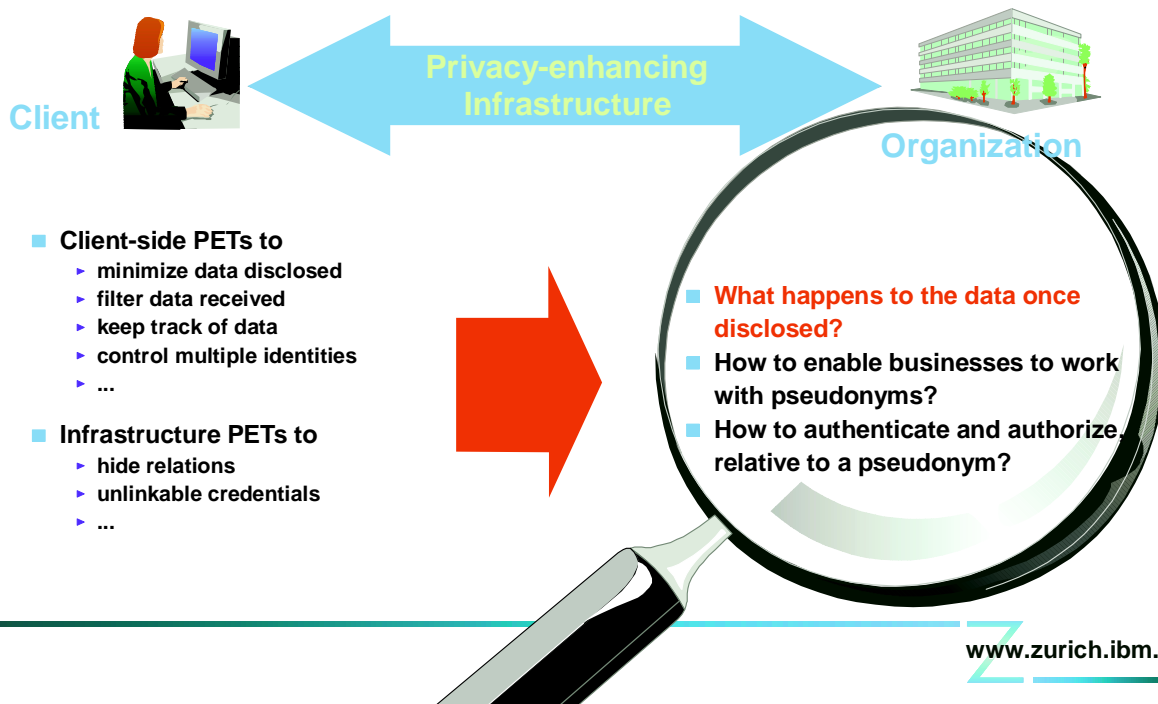
Satoshi Hada, IBM Research, Tokyo

Günter Karjoth, Matthias Schunter, IBM Research, Zurich

P3Pnext WS

www.zurich.ibm.com

Focus of our Research



www.zurich.ibm.com

2b. E-P3P Applications and Non-Goals

Enforcement

Privacy Control:

- ▶ Preventing applications & employees from violating privacy

Audit

Privacy Violation Detection:

- ▶ Off-line check whether privacy has been violated

Transfer

Privacy Envelopes:

- ▶ Transfer of policy-protected data

User-interface

Use text or P3P instead:

- ▶ Displaying Privacy Preferences
- ▶ Collecting consent

 www.zurich.ibm.com

1a. Privacy-enabled Data Management

Current situation

- ▶ Enterprises cannot give privacy guarantees
- ▶ Customers hesitate revealing personal data
- ▶ Legal problems; no business



Enterprises need to

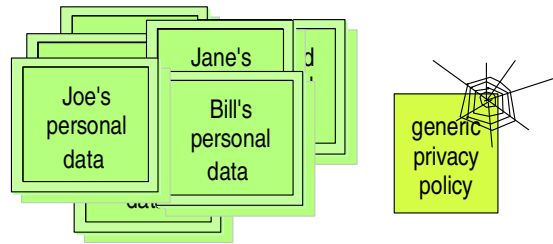
- ▶ Adhere to legal regulations
- ▶ Obtain consent before using personal info
- ▶ Only use the data for consented purposes
- ▶ Enable the customers to retain control

 www.zurich.ibm.com

1b. The Sticky Policy Paradigm

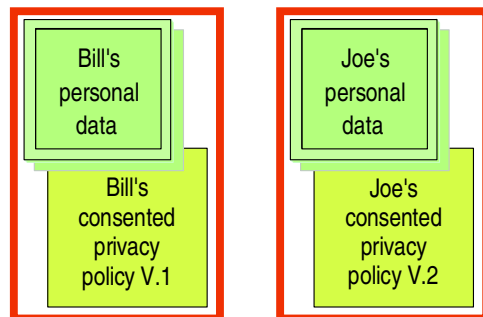
Today: (at most) one policy

- "Let's use these data for marketing!"
- "Wait a second, I'll update the policy..."



The future: sticky policy paradigm

- "Check the policy if marketing has been consented by this particular customer..."
- "If not, we ask for consent first"



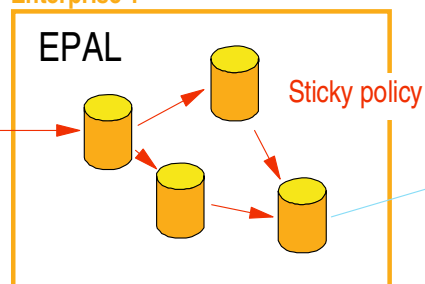
www.zurich.ibm.com

1c. Enterprise Privacy Policies

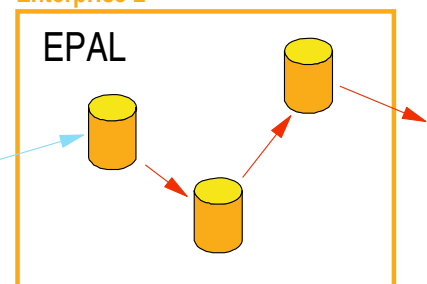


P3P
and/or
text

Enterprise 1



Enterprise 2

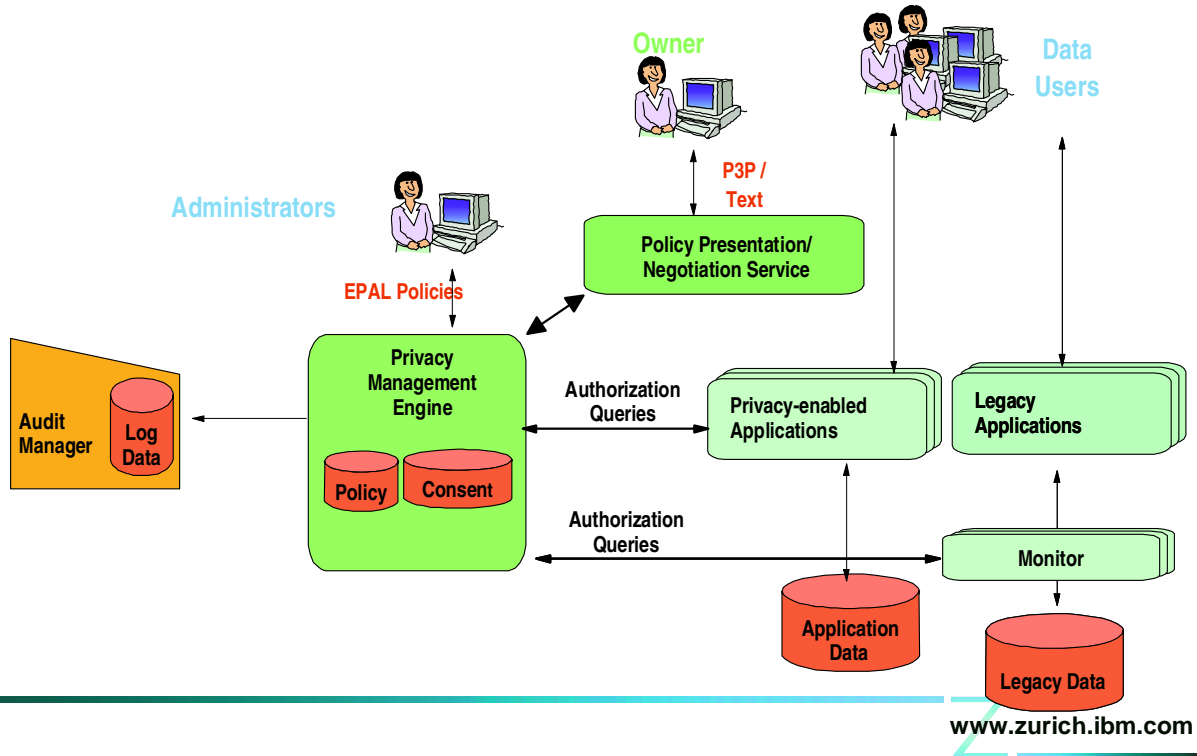


EPAL policy

- EPAL defines policy terminology and authorization rules
- Rules allow/deny privacy relevant actions, depending on purpose
- Can be mapped to P3P, supporting consistent internal/external views

www.zurich.ibm.com

1d. Privacy Enforcement Architecture



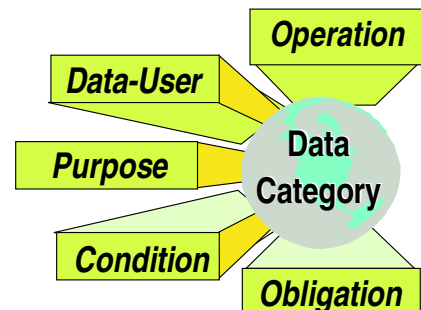
2a. EPAL by Example

Privacy promise:

- ▶ "Email can only be used for the book-of-the-month club *if consent has been given and age is more than 13*":

EPAL rule:

- ▶ <ALLOW
 data-user="borderless-books"
 data-category="email"
 purpose="book-of-the-month-club"
 operation="read"
 condition="/CustomerRecord/Consent/BookClub=True
 && /CustomerRecord/age>13">



From Privacy Promises to Enforcement

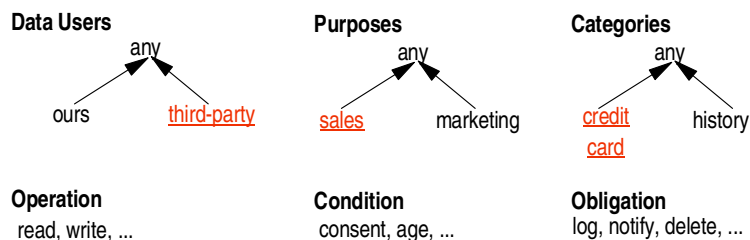
Elements	P3P	EPAL
Categories	list; predefined	hierarchy
Data-Users	list; predefined	hierarchy
Purposes	list; predefined	hierarchy
Operations	'use'	list
Conditions	none	yes
Obligations	'retention'	yes
Choices	+/- purpose	generalized
Deployment	none	cross-application
Conclusion	<ul style="list-style-type: none"> ✓ Simple ✓ Interoperable ✗ Non-extensible ✗ Limited ✗ Sector-specific 	<ul style="list-style-type: none"> ✓ Privacy Control ✓ Interoperable within each Sector

www.zurich.ibm.com

2b. EPAL Syntax

Elements: EPAL element definitions define scope:

- ▶ Data users, purposes, and categories are **hierarchies**
- ▶ Operations, obligations, and conditions are **lists**



Rules: EPAL rules authorize access:

- ▶ (d-category, d-user, purpose, operation, condition, obligation)

www.zurich.ibm.com

2b. Example: An EPAL Rule in XML

```
▶ <rule id="rule1" precedence="5" ruling="allow">
  ♦ <short-description>Models Par 8 of HIPPA
    law.</short-description>
  ♦ <data-user id="sales"/>
  ♦ <data-category id="financial"/>
  ♦ <purpose id="email marketing"/>
  ♦ <action id="read"/>
  ♦ <condition id="consentToMarketing"/>
  ♦ <obligation id="retention">
    <parameter id="days">5</parameter>
  </obligation>
▶ </rule>
```

2c. EPAL Semantics

Inheritance:

- ▶ Allow inherits down along hierarchies
- ▶ Deny inherits up and down (group-like)

Processing request (d-category, d-user, purpose, operation)

- ▶ Check whether there exists applicable rule(s)
 - ♦ that cover request directly or by inheritance
 - ♦ have satisfied condition(s)
- ▶ Decide:
 - ♦ Allow and deny rules → Ignore allow rules
 - ♦ Either Allow or deny rules → Choose one for ruling + obligations
 - ♦ No rule → Default ruling (with no obligations)

2c. EPAL Semantics

Inheritance:

- ▶ Allow inherits down along hierarchy
- ▶ Deny inherits up and down (group-like)

EPAL gives abstract vocabularies --
we also need deployment descriptions!

Processing request (d-category, d-user, purpose, operation)

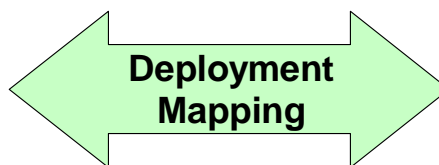
- ▶ Check whether there exists applicable rule(s)
 - ◆ that cover request directly or by inheritance
 - ◆ have satisfied condition(s)
- ▶ Decide:
 - ◆ Allow and deny rules → Ignore allow rules
 - ◆ Either Allow or deny rules → Choose one for ruling + obligations
 - ◆ No rule → Default ruling (with no obligations)

 www.zurich.ibm.com

Deploying Vocabularies

Application-specific Terms

- ◆ application + task
- ◆ storage location
- ◆ data
- ◆ credentials
- ◆ operation
- ◆ (stored) procedures



(Privacy) Policy Terms

- ◆ (purpose)
- ◆ data-user
- ◆ data-category
- ◆ (privacy) action
- ◆ condition
- ◆ obligation

Requirements:

- ▶ Application-independent Policies 'CPO driven'
- ▶ Enforce this policy across multiple applications

Problems:

- ▶ Applications should not know the policy
- ▶ Applications use their own terminology
- ▶ Applications know nothing about 'purposes'

 www.zurich.ibm.com

References and Contact



Questions?

IBM Privacy Institute

- ▶ <http://www.research.ibm.com/privacy/>

IBM Zurich Research Lab

- ▶ <http://www.zurich.ibm.com/>

How to reach us:

- ▶ wmi@zurich.ibm.com
- ▶ [\(+41\) 1 724 8220](tel:+4117248220)

 www.zurich.ibm.com