

Privacy Manager



Tivoli

Dr Paul Ashley
Austin, Texas, USA
paul.ashley@tivoli.com

Overview

- Who am I?
- What is Tivoli?
- Problem – Privacy!
- Tivoli Solution : Privacy Manager

Who am I?

Tivoli

Who am I?

- **Senior Security Architect**
 - Tivoli SecureWay
 - PhD in network security architectures
- **My scope**
 - Working with Product Development
 - Future product features, input from customers
 - Customers
 - Financial, Telecommunications, Manufacturing

What is Tivoli?



What is Tivoli

- Tivoli is the “management software” arm of IBM
- Includes security management
 - Application security management – Policy Director
 - Privacy Manager is part of this family
 - Event notification management – Risk Manager
 - Others ...
Tivoli SecureWay

The Tivoli logo consists of the word "Tivoli" in a white, bold, sans-serif font, set against a red rectangular background with a slight 3D effect.

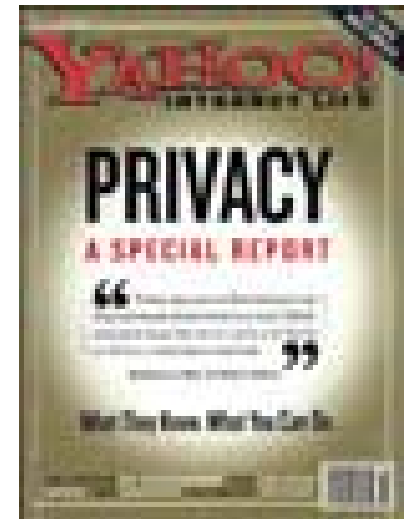
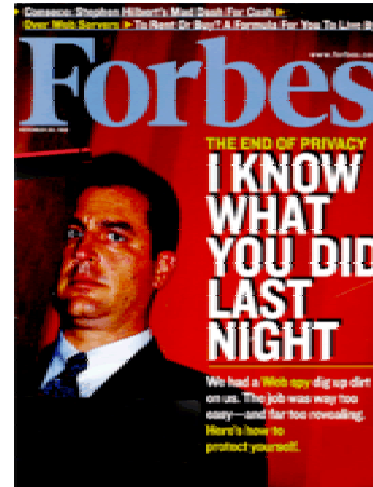
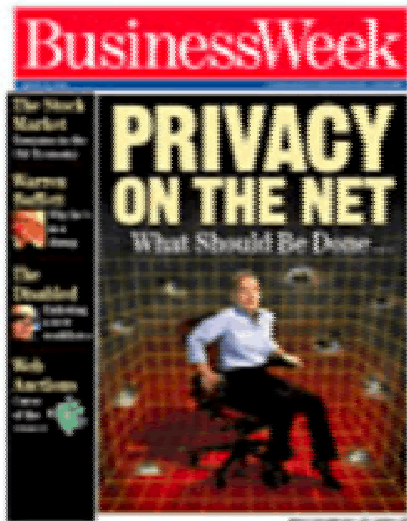
Manage. Anything. Anywhere.™

A smaller version of the Tivoli logo, featuring the word "Tivoli" in white on a red background, positioned in the bottom right corner of the slide.

Problem – Privacy!



Privacy in the Headlines



Privacy Concerns for Consumers

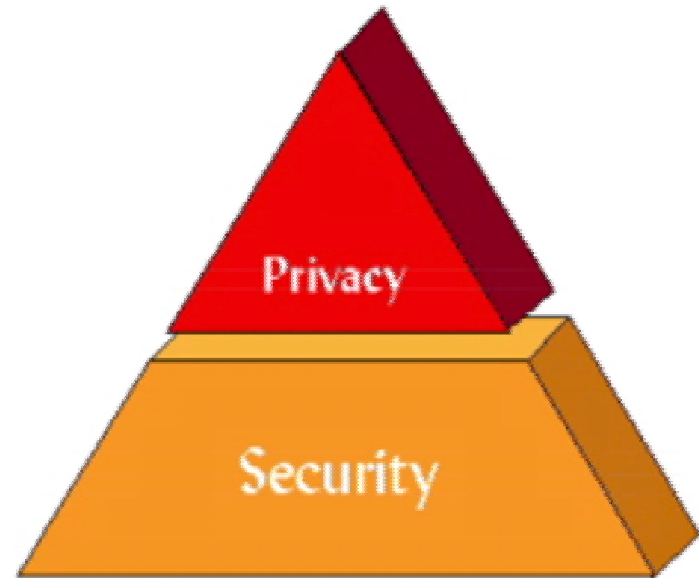
- The risks come from using information collected for one purpose in ways unknown and unapproved by the consumer....
 - Loss of anonymity
 - Profiling
 - Ease of access to the social security #
 - Identity theft
 - Collection of children's personal data
 - Junk mail & telemarketers
 - Misuse of health information, financial information & personal communications.

Privacy Concerns for e-Business

- Complying with government regulations
- Risk to brand if lose consumer trust
- Legal liability
- Lost revenue
- PR Nightmare

Fair Information Practices

- Notice
- Choice
- Access
- Security



Only 20 percent of [web] sites were found to have implemented all four fair information practices. (FTC survey 5/00)

Impact of Privacy Concerns and Violations

- Two thirds of Web users are concerned about their privacy. As a result, they spent \$2.8 billion less online than they otherwise would have in 1999.
(Forrester, 9/99)
- “Regulatory action ... is a very real danger for online violators, but the more serious danger may be to the bottom line in situations where consumer trust is shaken by a public outing.”
(Giga Information Group, June 6, 2000)

Privacy Regulation

- Europe: European Union Directive 95/46/EC
- Pacific Rim
 - Australian government considering legislation; Hong Kong, Taiwan, New Zealand have instituted privacy laws
 - Canada has instituted privacy laws.
- United States
 - EU and US discussions - “safe harbor”
 - HIPAA Security and Privacy Rules
 - COPPA - Children's Online Privacy Protection Act
 - FTC recommends legislation (5/22/00)

IBM/Tivoli's Role

- IBM internally
 - This year has appointed a Chief Privacy Officer to oversee IBM's own privacy policies
- Standards
 - Founding member of Online Privacy Alliance
 - Championed Privacy Leadership Initiative
 - Key role in creating P3P standard in W3C
 - Involved in other industry organizations such as ISTPA, CPEX
 - IGS Privacy Services

What Is P3P?

The Platform for Privacy Preferences Project (P3P), developed by the World Wide Web Consortium, is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. At its most basic level, P3P is a standardized set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P enabled browsers can "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P enhances user control by putting privacy policies where users can find them, in a form users can understand, and, most importantly, enables users to act on what they see.

Our Solution - Privacy Manager



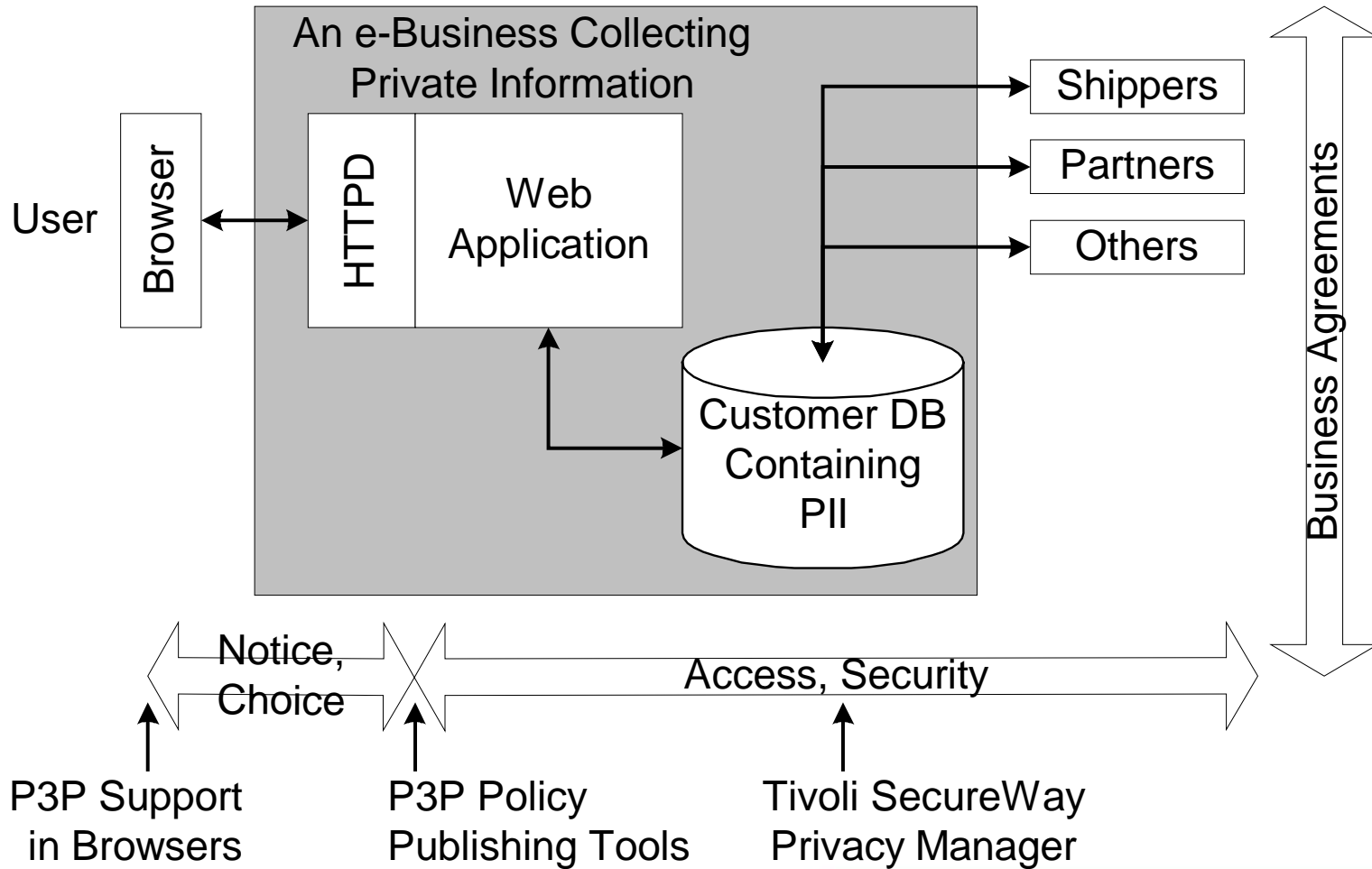
Tivoli SecureWay Privacy Manager

- Helps protect consumers' personally identifiable information (PII)
- Enforces access to data according to privacy policy

Privacy Manager Features

- Centralized administration of privacy policies regarding access to personally identifiable information (PII)
- Pre-defined privacy namespace and roles
- Rules engine supports dynamic roles
 - Enable access decisions to take into account the relationship between the requester and the subject of the data (e.g., self/subject, parent, primary care physician)
- Uses Policy Director authorization and audit features
- Sample Applications to get you off to a quick start

Web Privacy Overview



Methods of Deployment

- 1) Use predefined roles and ACLs to control access to specific URLs
- 2) Protect Web applications that use dynamic URLs
- 3) Use Privacy API and Roles Engine
 - To apply access control to fields
 - To make access decisions based on relationship between user and subject of data.

Extendable Privacy Manager PII Namespace

- /Personal/Location/Address
- /Personal/Location/Telephone
- /Personal/Location/Mail
- /Personal/Affiliation/Organizational
- /Personal/Affiliation/Political
- /Personal/Affiliation/Religious
- /Personal/Characteristics/RaceEthnicity
- /Personal/Characteristics/Gender
- /Healthcare/Mental Health/Psychiatric Notes
- /Healthcare/Mental Health/Psychiatric Diagnosis
- /Healthcare/Epidemiologic/HIV
- /Healthcare/Genetics
- /Healthcare/History of Care/Patient Record/Care Episode/Clinical Observation
- /Healthcare/History of Care/Patient Record/Care Episode/Abortion
- /Healthcare/History of Care/Patient Record/Care Episode/Substance-Abuse
- /Healthcare/History of Care/Patient Record/Care Episode/Prescription
- /Healthcare/History of Care/Patient Record/Care Episode/Medical Diagnosis
- /Legal/Criminal Record
- /Legal/Forensic/DNA
- /Legal/Forensic/Fingerprint
- /Legal/Forensic/Serology
- /Legal/Investigative/File
- /Financial/Credit History
- /Financial/Transaction History
- /Financial/Income
- /Financial/Assets/BankAccount
- /Financial/Insurance

Predefined Privacy Roles

- Personal
- Health Care
- Employer
- Government
- Law Enforcement
- Business Partner
- Financial
- Employee
- Process
- Audit
- P3P

Predefined Privacy Roles: Personal

- Personal-Subject
- Personal-NextOfKin
- Personal-AuthorizedAgent
- Personal-Executor
- Personal-ParentOfSubjectUnder13

Predefined Privacy Roles: Health Care

- **HealthCare-Provider**
- **HealthCare-ProviderClinical**
- **HealthCare-ProviderEmergency**
- **HealthCare-ProviderPrimary**
- **HealthCare-MentalHealthProvider**
- **HealthCare-MentalHealthProviderPrimary**
- **HealthCare-HealthcareProviderRegistration**
- **HealthCare-HealthcareProviderBusinessOffice**
- **HealthCare-HealthcareProviderClaimsProcessor**
- **HealthCare-HealthcareProviderMedicalRecsDept**
- **HealthCare-HealthcarePayer**
- **HealthCare-HealthcarePayerPlanAdmin**
- **HealthCare-HealthcarePayerClaimsProcessor**
- **HealthCare-HealthcareResearcher**
- **HealthCare-HealthPlan**
- **HealthCare-HealthcareClearinghouse**

Predefined Privacy Roles: Employer

- Employer-HRAdmin
- Employer-BenefitsAdmin

Predefined Privacy Roles: Government

- Government-TaxOfficial
- Government-Judge
- Government-CourtOfficer
- Government-SubpoenaHolder
- Government-CustomsOrImmigrationOfficer
- Government-PostalOfficer
- Government-CensusOfficer
- Government-Regulator

Predefined Privacy Roles: Law Enforcement

- LawEnforcement-Officer
- LawEnforcement-WarrantHolder
- LawEnforcement-CoronerOrMedicalExaminer
- LawEnforcement-Prosecutor
- LawEnforcement-LegalCounsel

Predefined Privacy Roles: Business Partner

- BusinessPartner-Marketer
- BusinessPartner-Retailer
- BusinessPartner-TelcoProvider
- BusinessPartner-Subcontractor
- BusinessPartner-Supplier

Predefined Privacy Roles: Financial

- Financial-Insurer
- Financial-Bank
- Financial-SecuritiesBroker
- Financial-CreditIssuer
- Financial-Realtor

Predefined Privacy Roles: Employee

- Employee-Employee
- Employee-HelpDesk
- Employee-CustomerServiceRep
- Employee-MfgOrShipping
- Employee-Accounting
- Employee-Sales
- Employee-Marketing

Predefined Privacy Roles: Process

- Process-Backup
- Process-BackupRestore
- Process-Anonymizer
- Process-DataAggregator
- Process-DataMiner

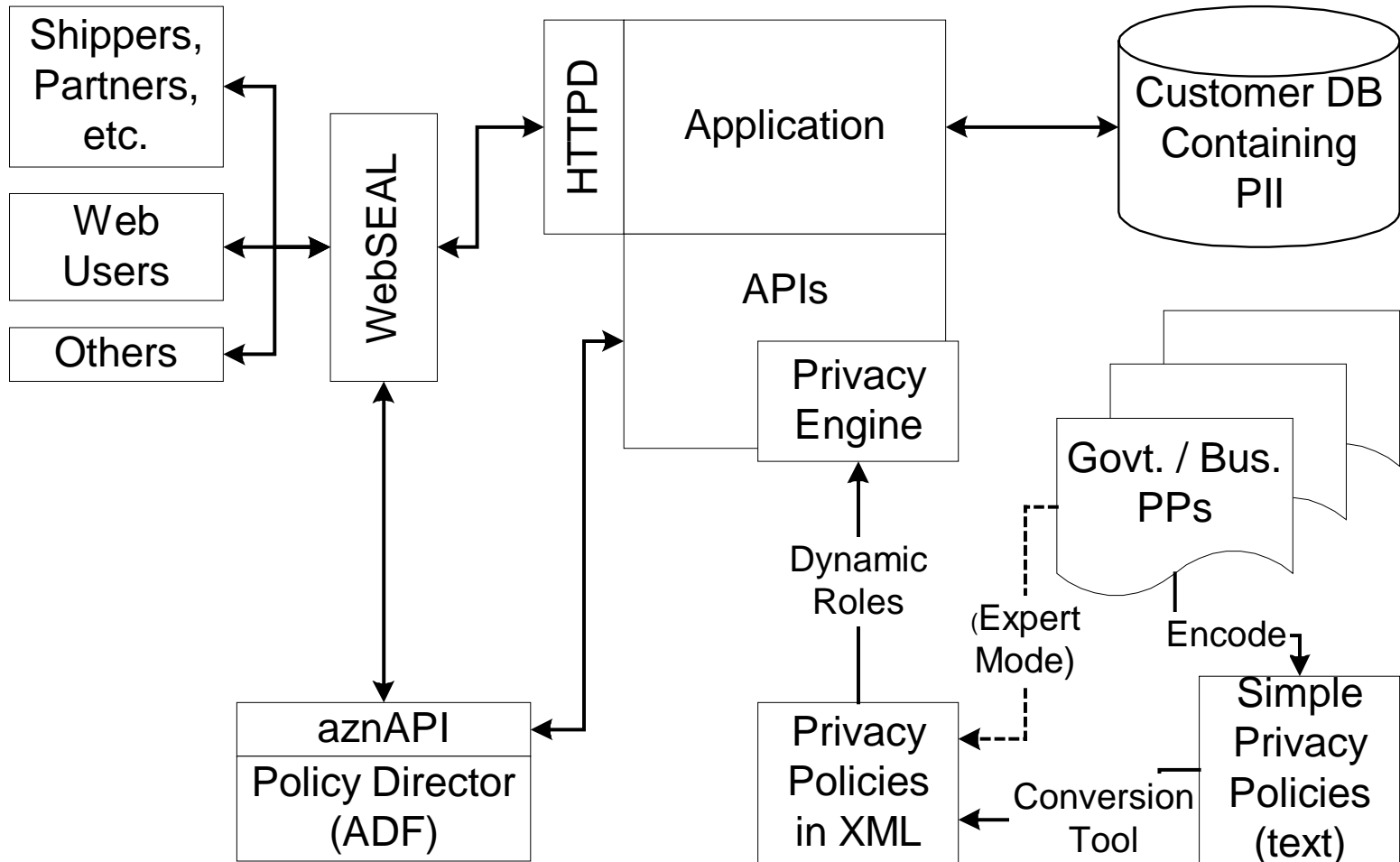
Predefined Privacy Role: Auditor

- Auditor-FinancialAuditor
- Auditor-SecurityAuditor
- Auditor-PrivacyAuditor

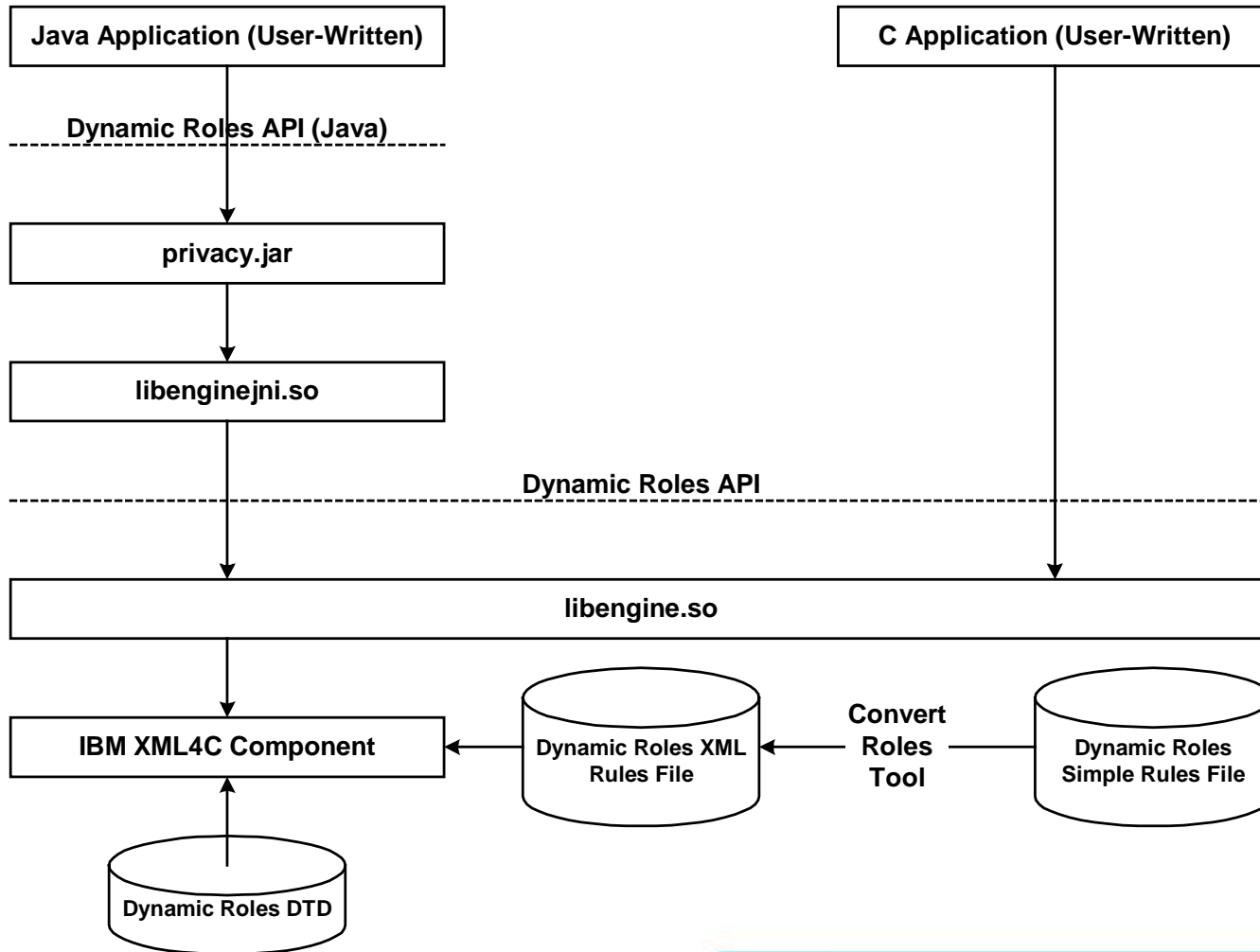
Predefined Privacy Roles: P3P

- p3p-Recipient-Ours
- p3p-Recipient-Delivery
- p3p-Recipient-Same
- p3p-Recipient-Other
- p3p-Recipient-Unrelated
- p3p-Recipient-Public

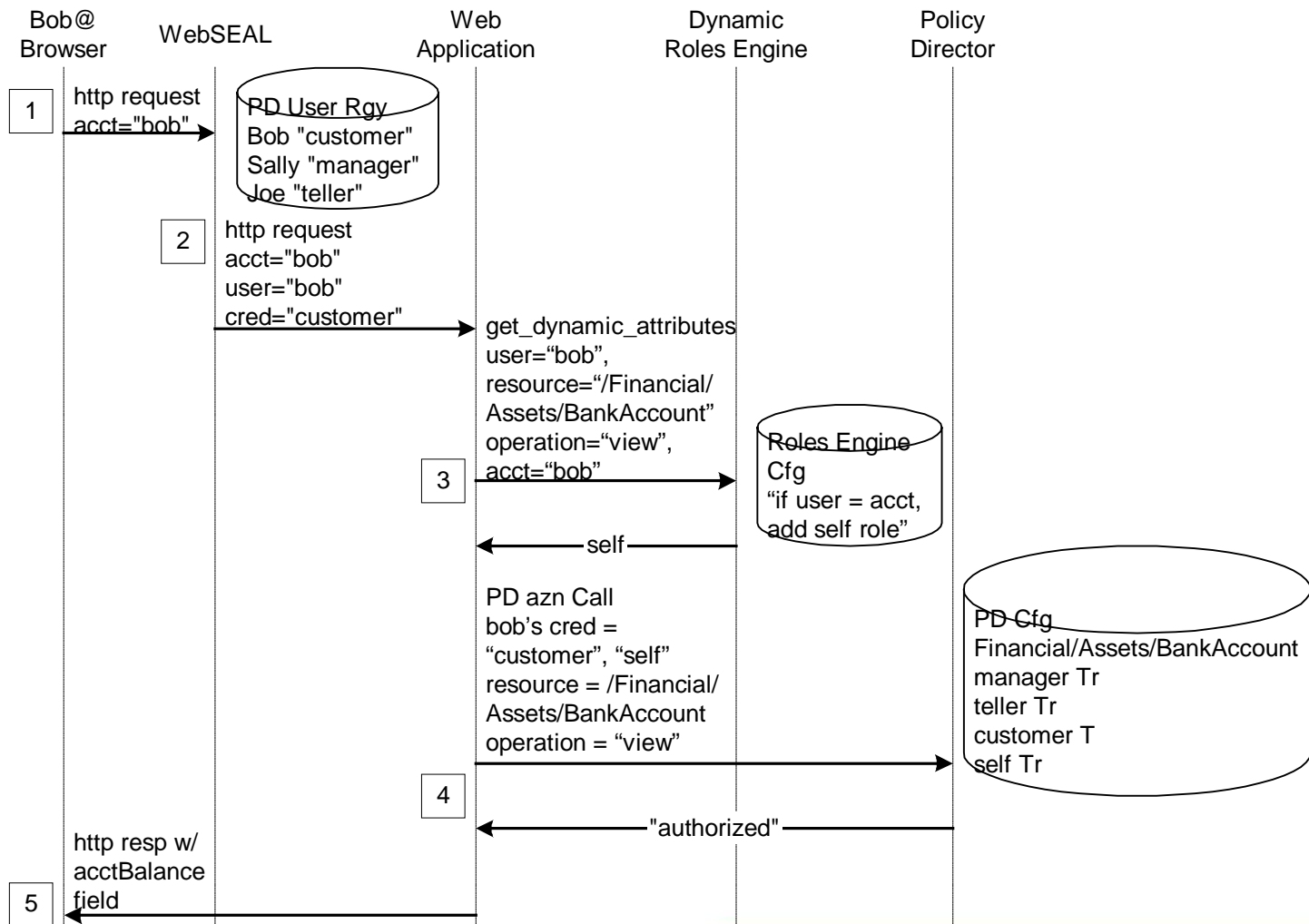
Roles Engine and Privacy API



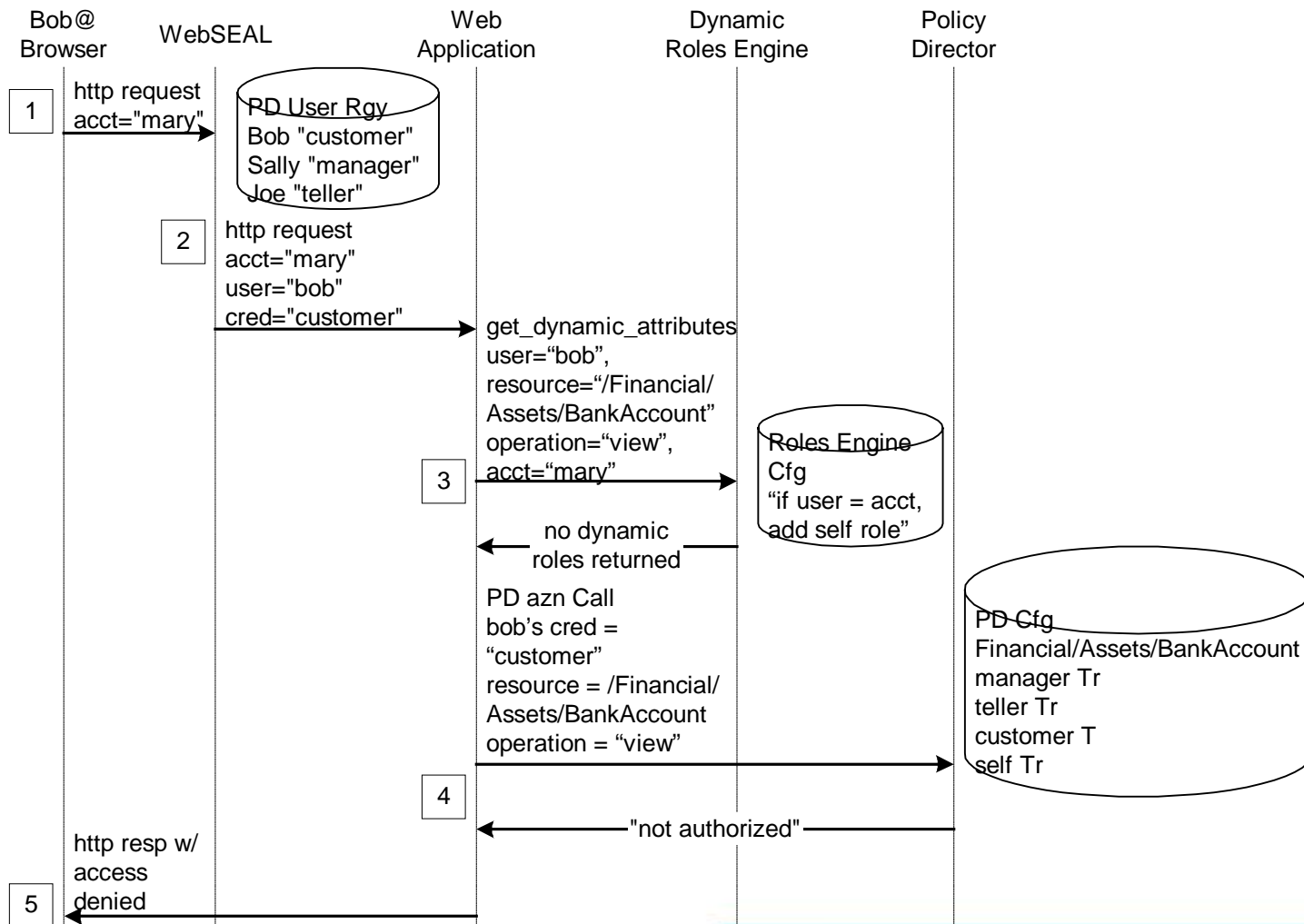
get_dynamic_attributes() Privacy API



Sample Scenario 1: Bob Can View His Bank Account Balance



Sample Scenario 2: Bob Cannot View Mary's Account Balance



Privacy Policy Definition

For those who like to see the code...

```
// get attributes from user's credential using aznAPI
attrlist = azn_creds_get_attrlist_for_subject (creds);

// Figure out what dynamic attributes the user is
// entitled to
dynattrs = get_dynamic_attributes (attrlist, resource,
operation);

// add dyn. roles to cred
azn_creds_modify(creds, dynattrs);
azn_decision_access_allowed (creds, resource, operation)
```

Management Console

The screenshot displays the Tivoli Policy Director Management Console interface. The title bar indicates the domain is `/.../custeng2_cell` and the user is logged in as `cell_admin`. The main window is divided into several sections:

- Protected Object Space:** A tree view on the left shows a hierarchy of objects. The `BankAccount` object under `Financial/Assets` is selected and highlighted in blue.
- Inherited ACLs:** A table on the right shows the ACLs inherited from the parent object `/Privacy/Financial/Assets/BankAccount`. The table has columns for ACLs, Type, ID, and Permissions.

ACLs	Type	ID	Permissions
BankAccount			
default-root			
default-privacy			
bank-account-access			
	any-authenticated		-----T-----
	group	AccountHolder	-----T-a-v-----
	group	AuthorizedPayee	-----T-a-----
	group	iv-admin	a-bc--T-----
	group	MyFinancialAdvisor	-----T-a-v-----
	group	Teller	-----T-a-v-----
	unauthenticated		-----T-----
	user	cell_admin	a-bc--T-----

At the bottom of the console, there is a **Bulletin Board** section.

Directions

- Technology isn't the "senior partner" in privacy
- Feedback from first users and continued involvement in industry organizations will be critical
- In general: Enhanced support for evolving standards and technologies

For More Information

- <http://www.tivoli.com/security>
- <http://www.w3.org/P3P>

Questions?

Tivoli Secure Way



Manage. Anything. Anywhere.™