IBM Security & Privacy Update

July 23, 2001

Anne Lescher
lescher@us.ibm.com

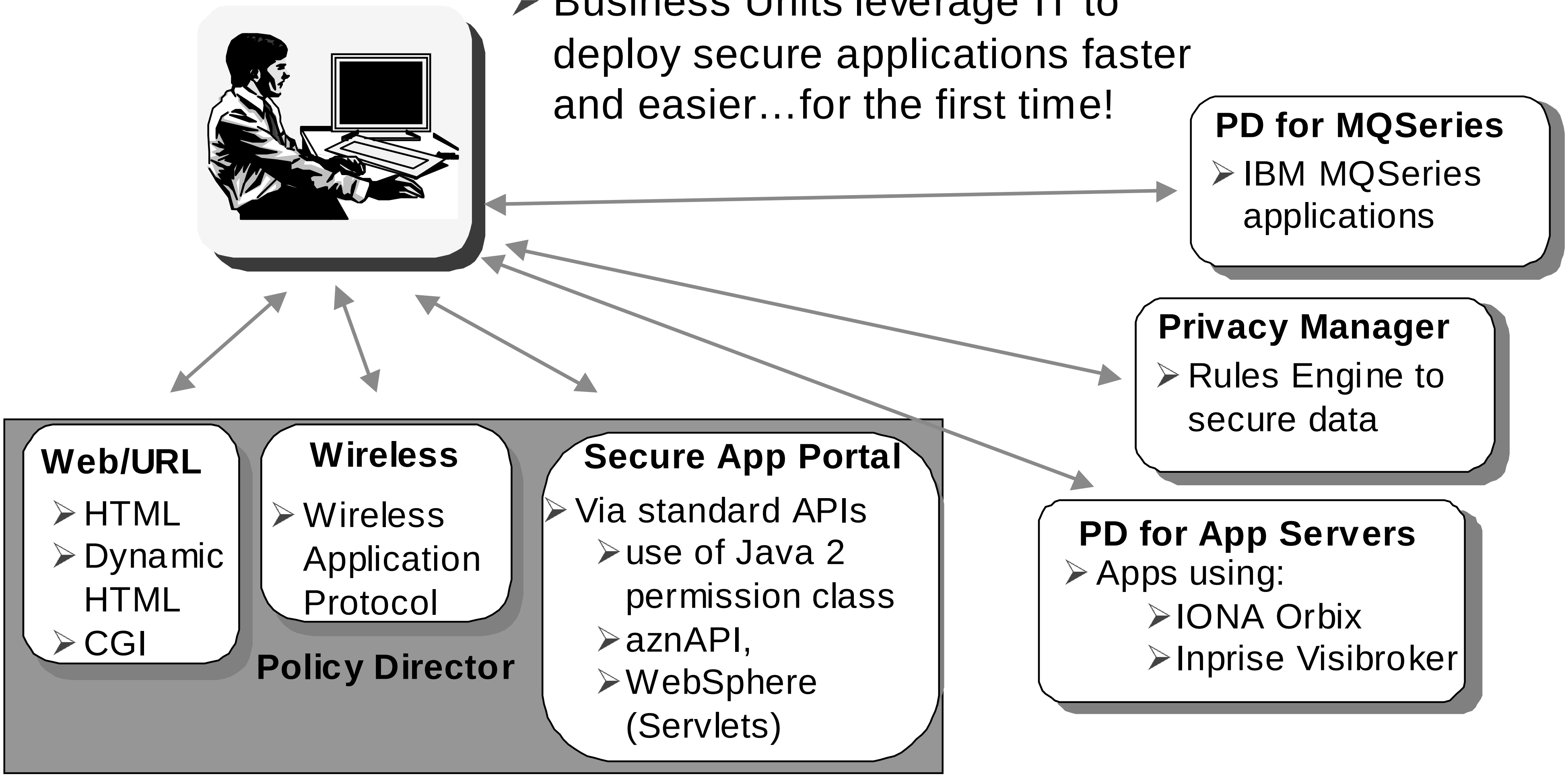
Hot Topics and Product Updates

- Policy Director
- PD MQSeries
- Enterprise Privacy Architecture
- Tivoli SecureWay Privacy Manager
- Real Time Intrusion Detection
- z/OS SecureWay Security Server
- Linux Security
- Cryptography
- Others: Wireless Security, User Identification

Policy Director Family

Establishes Security as an Enabler for e-business

- Business Units leverage IT to deploy secure applications faster and easier…for the first time!



PD for MQSeries

- IBM MQSeries applications

Privacy Manager

- Rules Engine to secure data

PD for App Servers

- Apps using:
  - IONA Orbix
  - Inprise Visibroker

Web/URL

- HTML
- Dynamic HTML
- CGI

Wireless

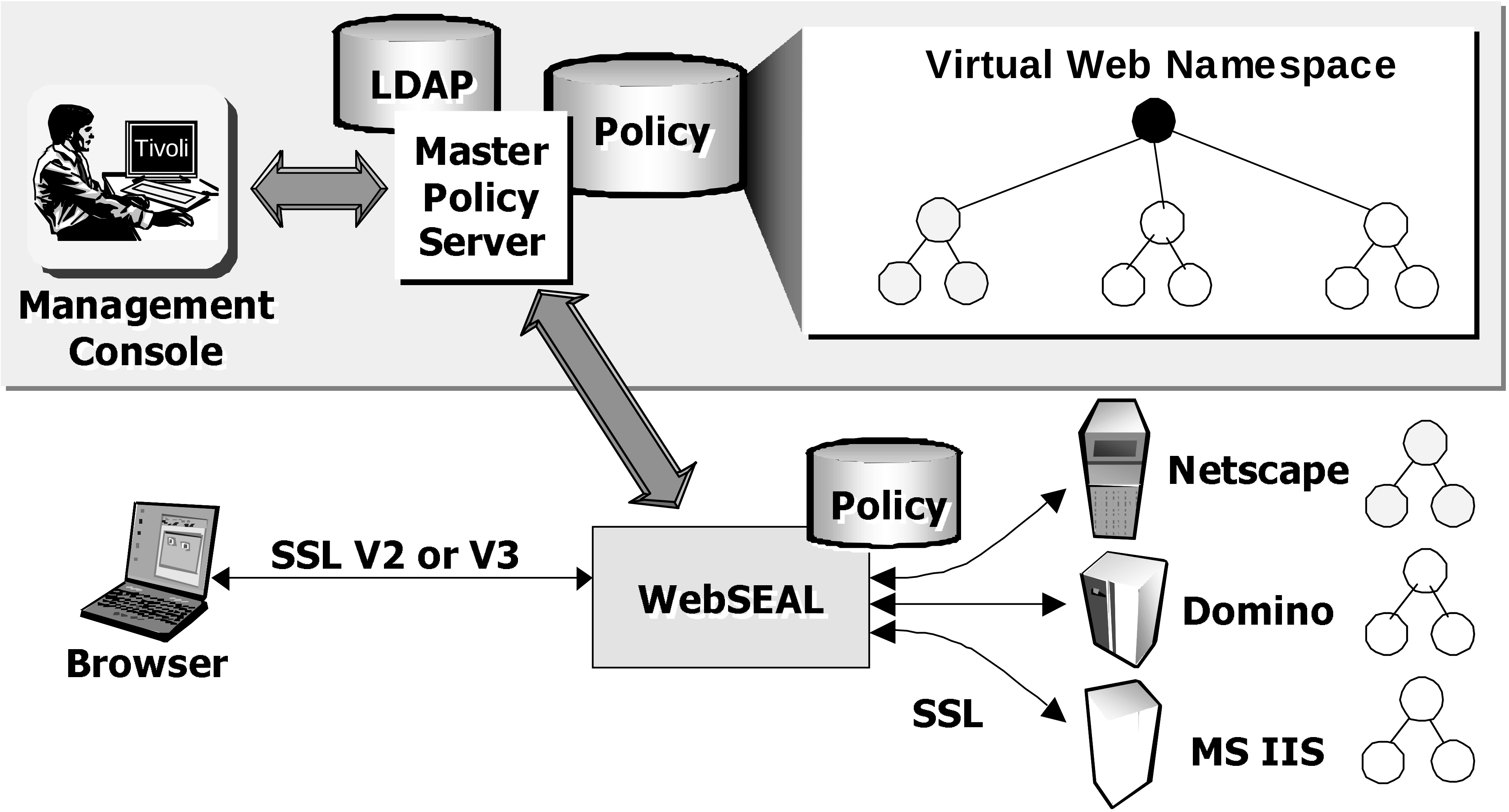
- Wireless Application Protocol

Secure App Portal

- Via standard APIs
  - use of Java 2 permission class
  - aznAPI,
  - WebSphere (Servlets)

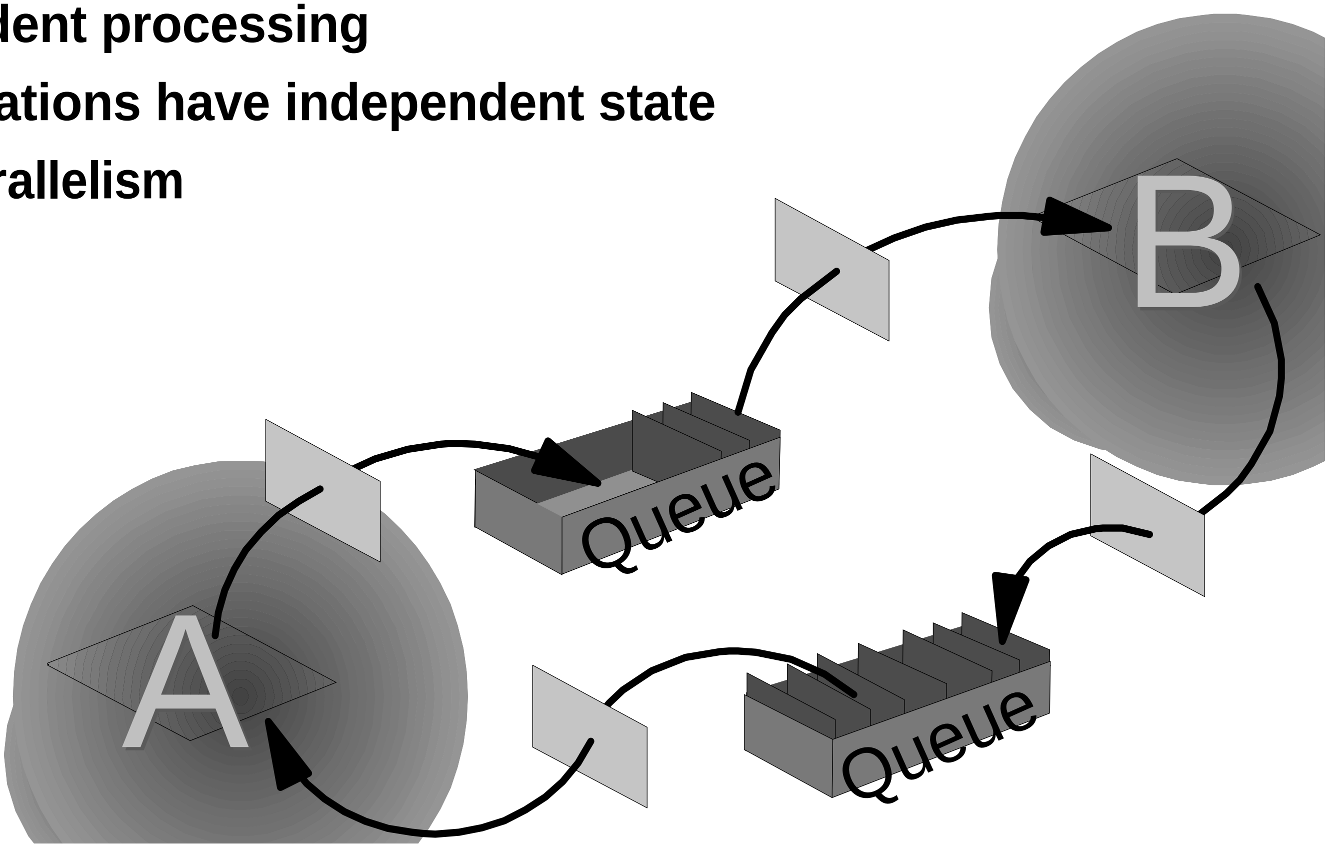
Policy Director

Policy Director WebSEAL



MQSeries Commercial Messaging

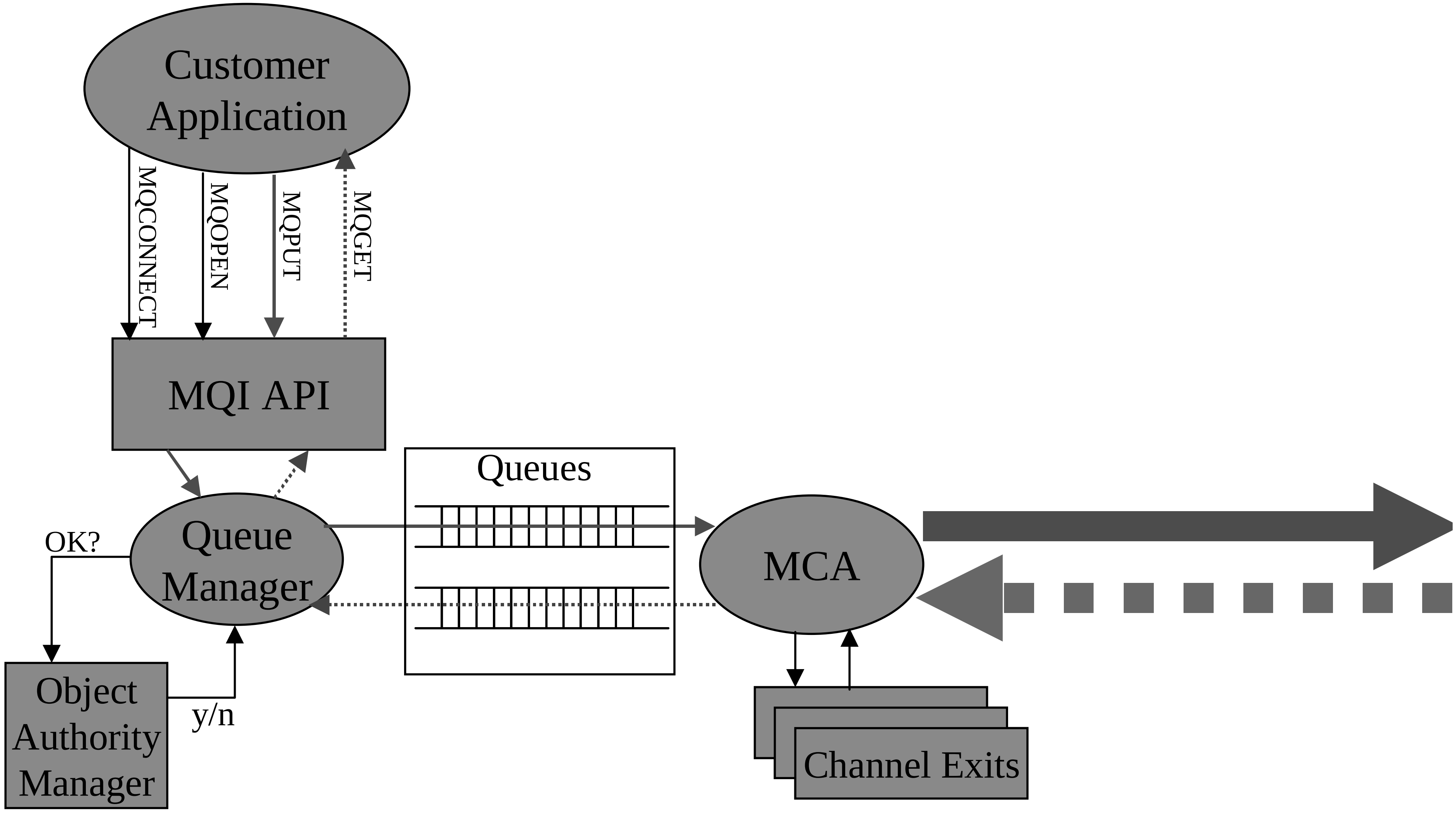
- Simple, multi-platform API
- Assured message delivery
- Time independent processing
- Partner applications have independent state
- Application parallelism



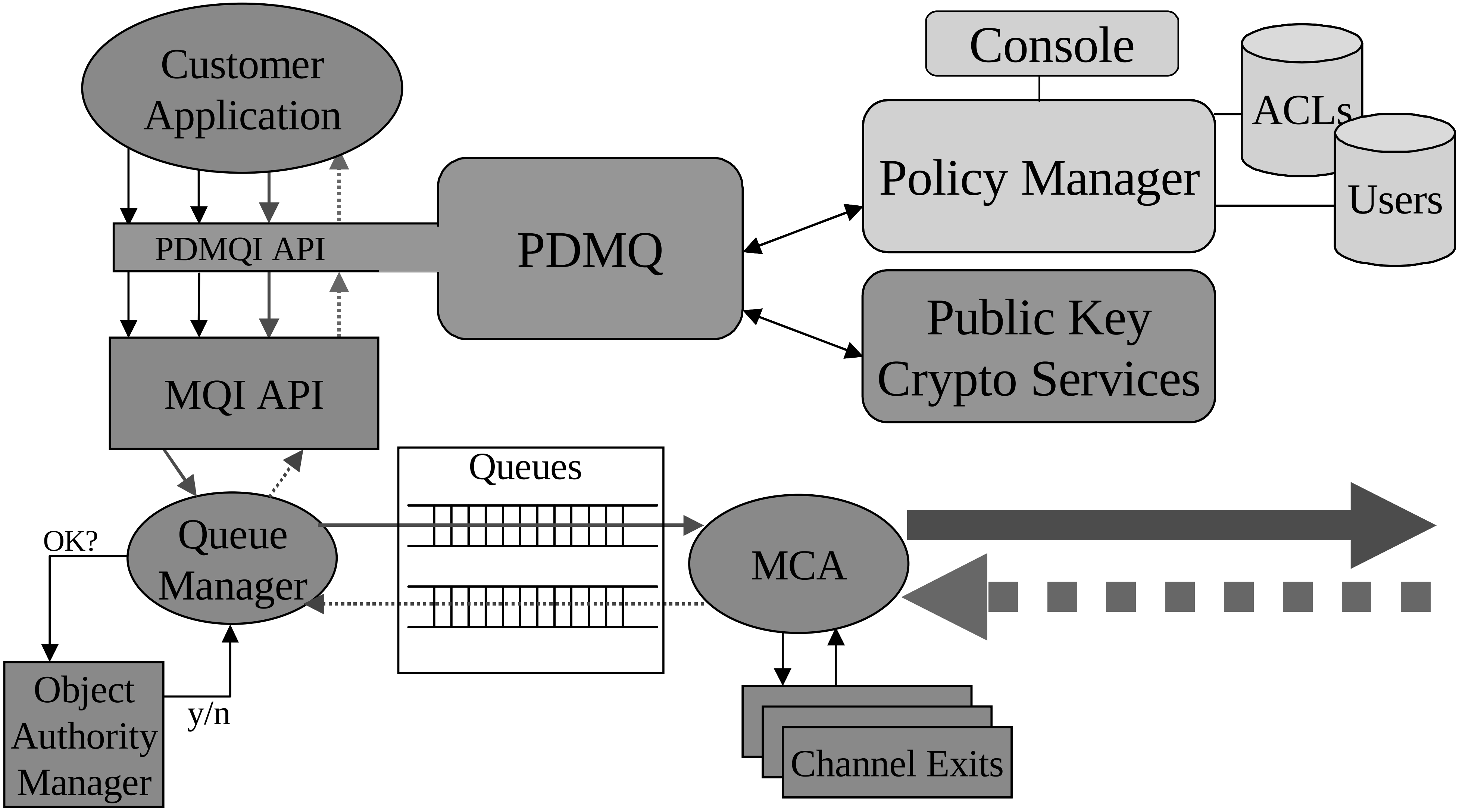
Policy Director for MQSeries

- Data protection and centralized access control for application based on IBM MQSeries
  - Let only the right people/tasks access a queue
  - Protect data while in queues and in transit
  - Cost effectively manage policy definition and enforcement
  - Support existing and new MQ Series applications without modification

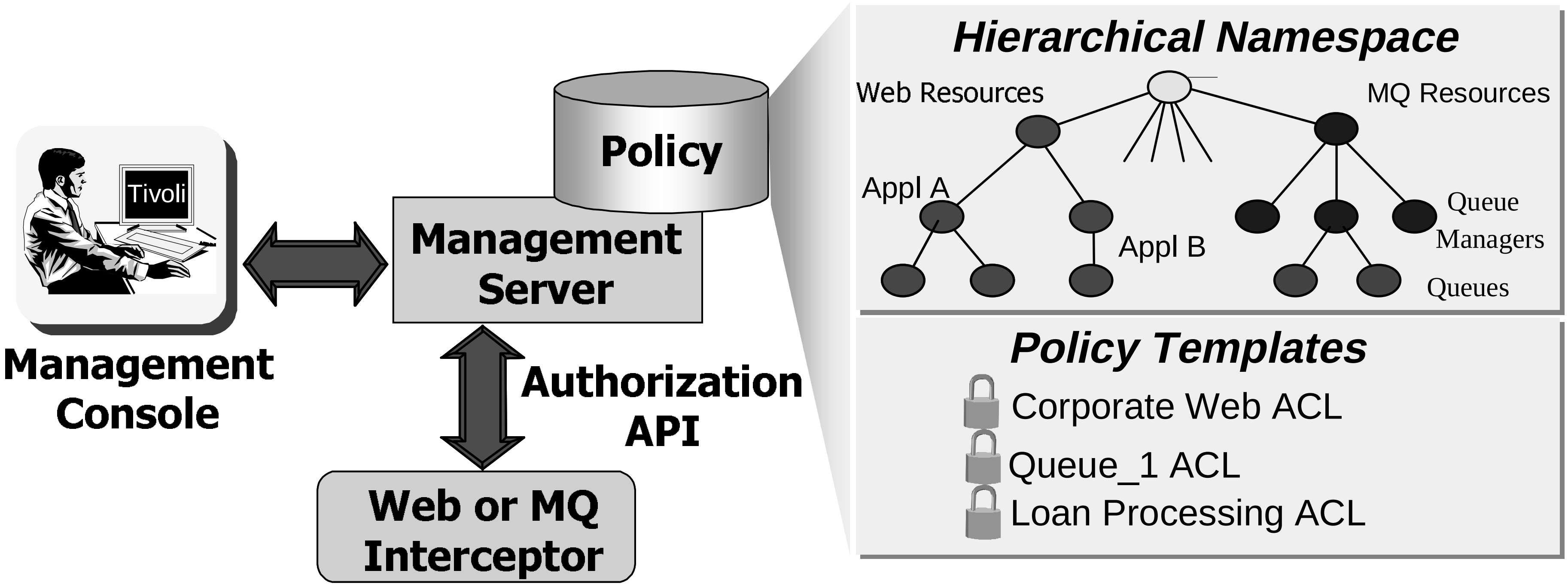
Standard MQ Series



MQ Series with Policy Director for MQ Series



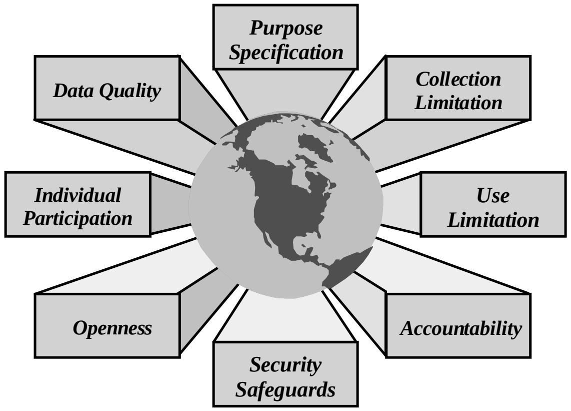
Policy Authorization



- API removes the need for authorization code in each application
- Management console
  - **Defines users and groups**
  - **Defines access control policy (ACLs)**
  - **Associate ACLs with objects in the hierarchical namespace**

Definition of Privacy

- Privacy as a fundamental right of self-determination [Westin 67]
  - The right of individuals to determine for themselves when, how, and to what extent information about them is communicated to others.
- Fair Information Practices
  - Notice, Access, Choice and Consent, Recourse, Security
- The OECD Principles [OECD 81]



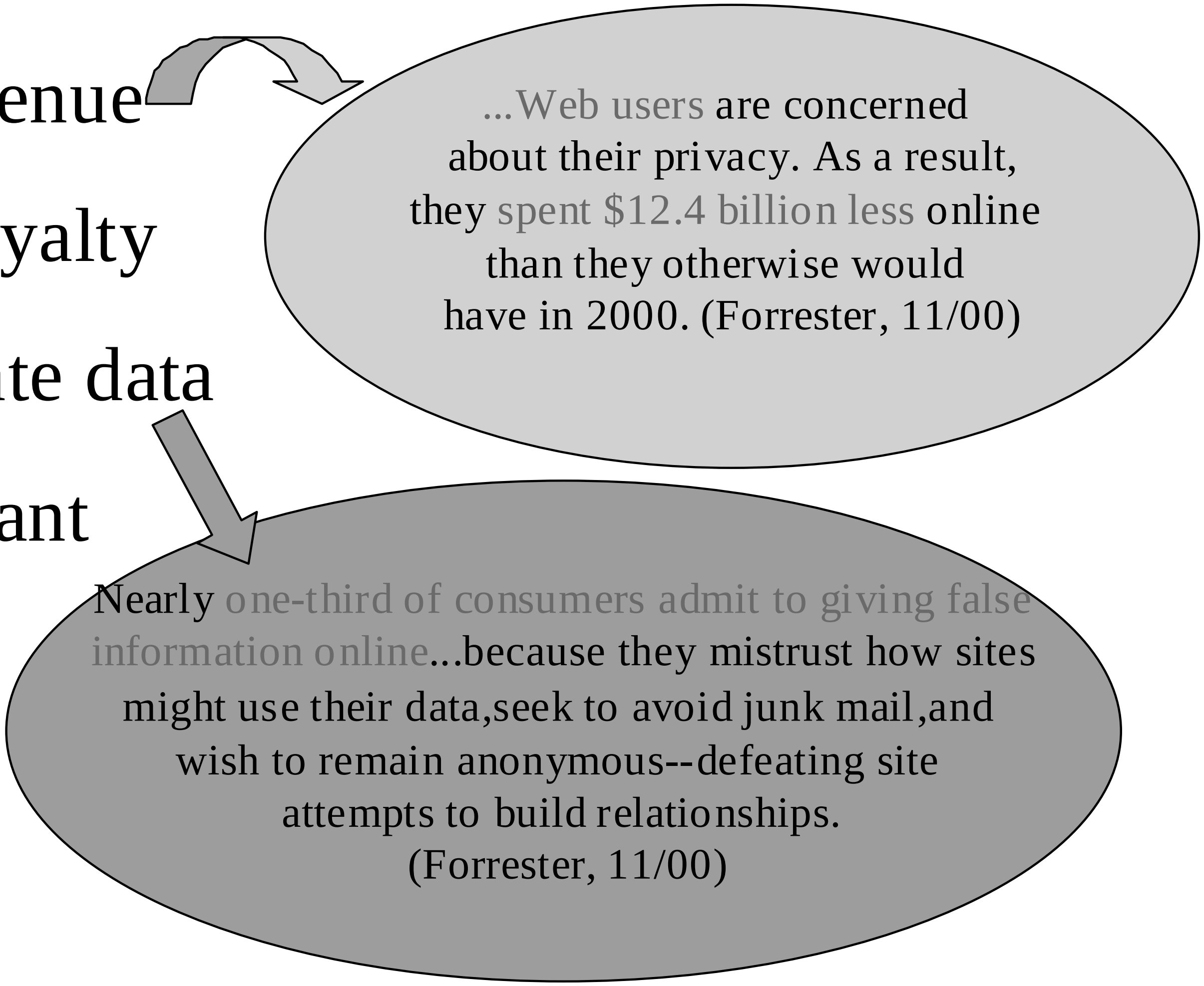
- Subject: Personally identifiable information.
- Purpose specification always required prior to collection.
- Individual's consent is always required prior to collection.
- Proportionality of collection, use, and retention.
- Openness, access, corrections.

Legislation in the United States

- Financial institutions
  - Must comply with Gramm-Leach-Bliley Act by July 2001
  - Need to respect their customers’ opt-out choices
- Healthcare organizations
  - Must comply with HIPAA privacy rules by Apr 2003
  - Security rules are expected to be finalized this year
- Government
  - e-government applications must be careful not to disclose SS# or other personal information

Consumer Concerns & The Impact

- Slower growth in revenue
- Reduced customer loyalty
- Provision of inaccurate data
- Withholding of relevant information



...Web users are concerned about their privacy. As a result, they spent $12.4 billion less online than they otherwise would have in 2000. (Forrester, 11/00)

Nearly one-third of consumers admit to giving false information online...because they mistrust how sites might use their data,seek to avoid junk mail,and wish to remain anonymous--defeating site attempts to build relationships. (Forrester, 11/00)

Decision Points in Selecting a Privacy Tool

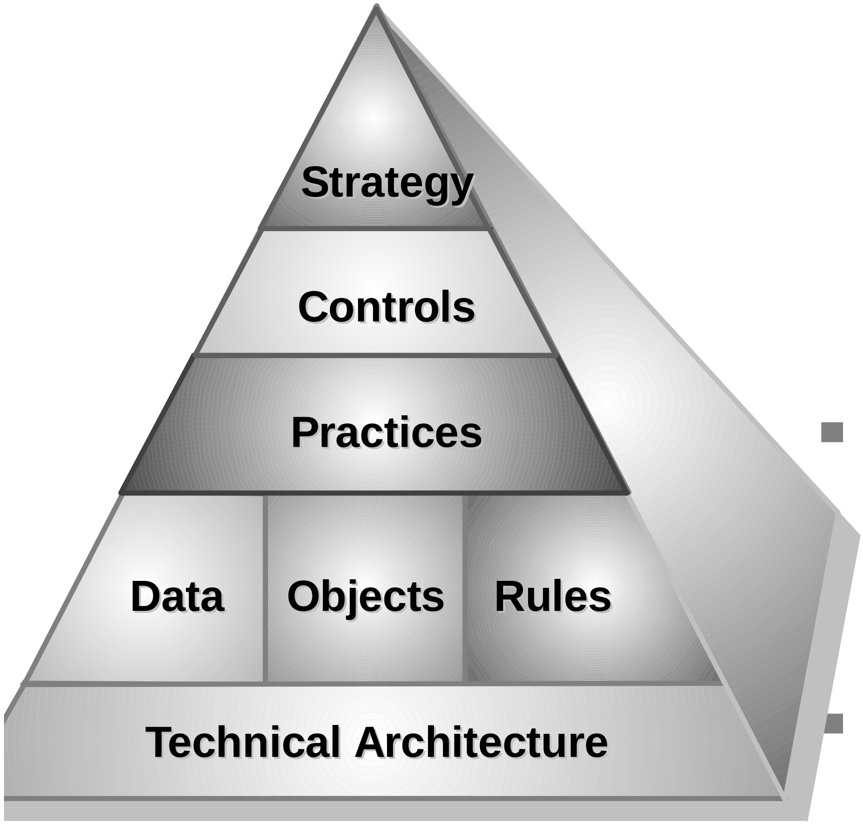
- Manage privacy policy compliance in application code, or in an external management and enforcement engine?
- Manage privacy by marking all sensitive data, or by controlling the process of accessing sensitive data?
  - Will a “marked data” approach require you to edit all your data bases, if your privacy policy changes?
- Manage privacy coordinated with security, or as a separate practice?

Your privacy policy may need to change in response to new laws, industry regulations, or marketing needs.

Customer Privacy Requirements

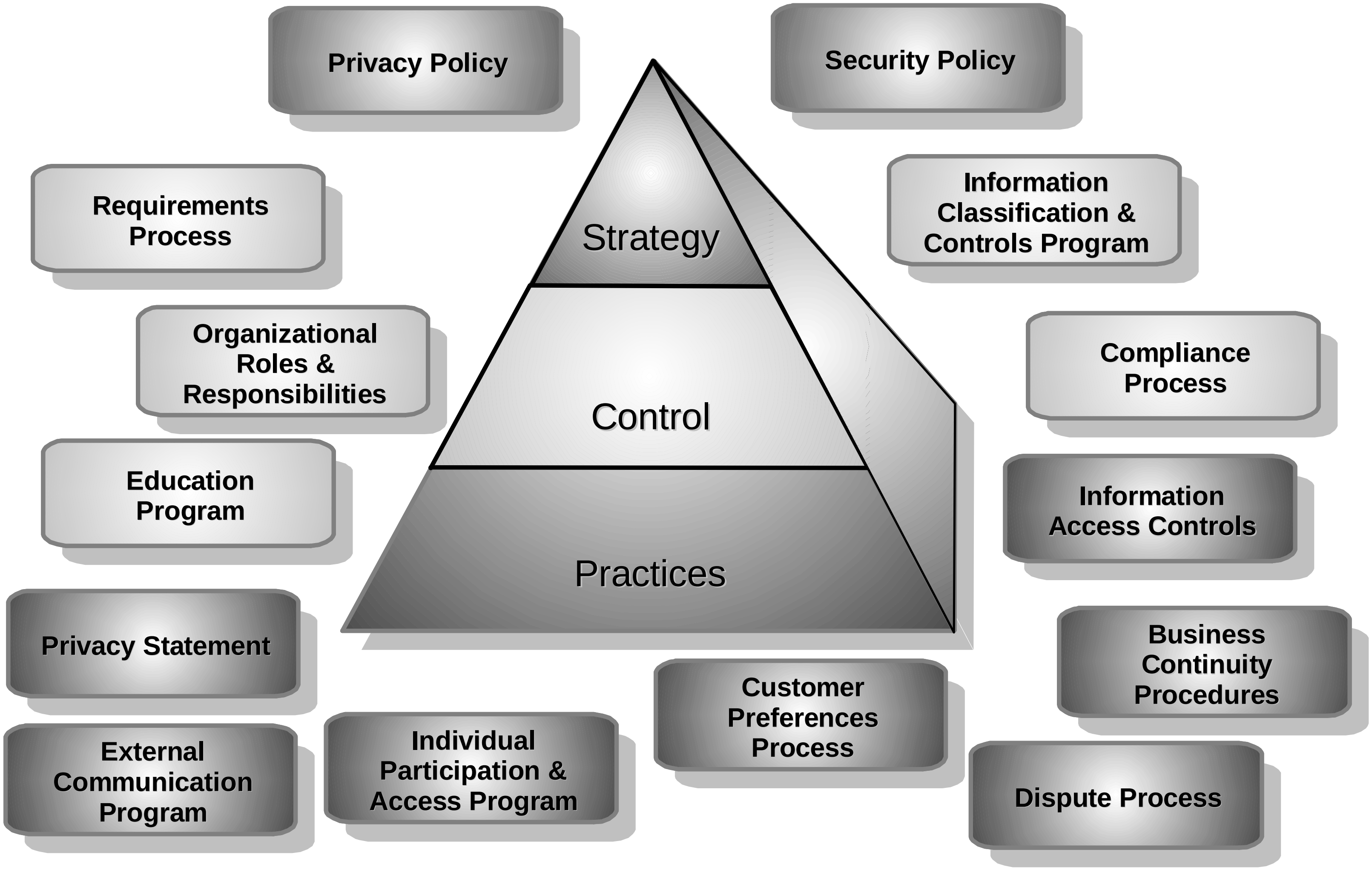
- Consistently enforce privacy policy
- Automate adherence to consumers’ opt-out or opt-in decisions (Choice)
- Implement controls so consumers can access to their own data (Access)
- Ensure data is used for the purpose(s) stated to or agreed upon
- Ensure data is protected from unauthorized access or alteration.
- Need audit trail of accesses to personal information

IBM's Enterprise Privacy Architecture



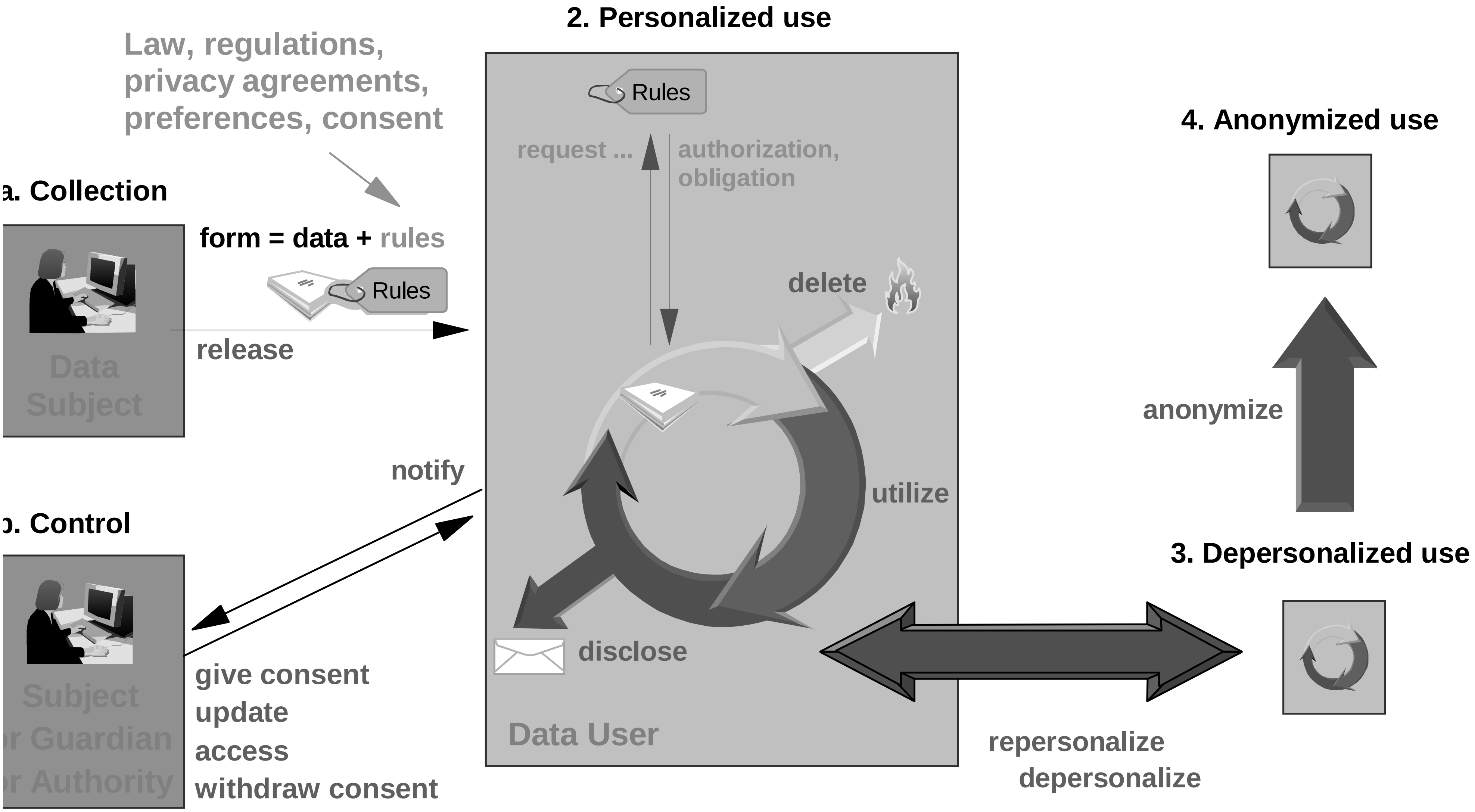
- Enterprise perspective
  - Leverage personal information **and** protect individual privacy
  - Build management systems and controls to integrate regulatory conditions into business processes
  - Roadmap for achieving privacy objectives
- Comprehensive
  - Strategy and organization
  - Processes
  - Technology
- Client driven
  - Compliance with multiple-regulations
  - Privacy as a competitive differentiator
  - Privacy enable business initiatives (CRM, Call Center, BI, etc.)

EPA - Management Infrastructure



Privacy Policy
Security Policy
Requirements Process
Strategy
Information Classification & Controls Program
Organizational Roles & Responsibilities
Control
Compliance Process
Education Program
Information Access Controls
Practices
Privacy Statement
Business Continuity Procedures
Customer Preferences Process
External Communication Program
Individual Participation & Access Program
Dispute Process

EPA - Generic Process Model



2. Personalized use

Law, regulations, privacy agreements, preferences, consent

Rules

request ...

authorization, obligation

4. Anonymized use

a. Collection

form = data + rules

Rules

delete

release

Data Subject

anonymize

notify

utilize

b. Control

3. Depersonalized use

disclose

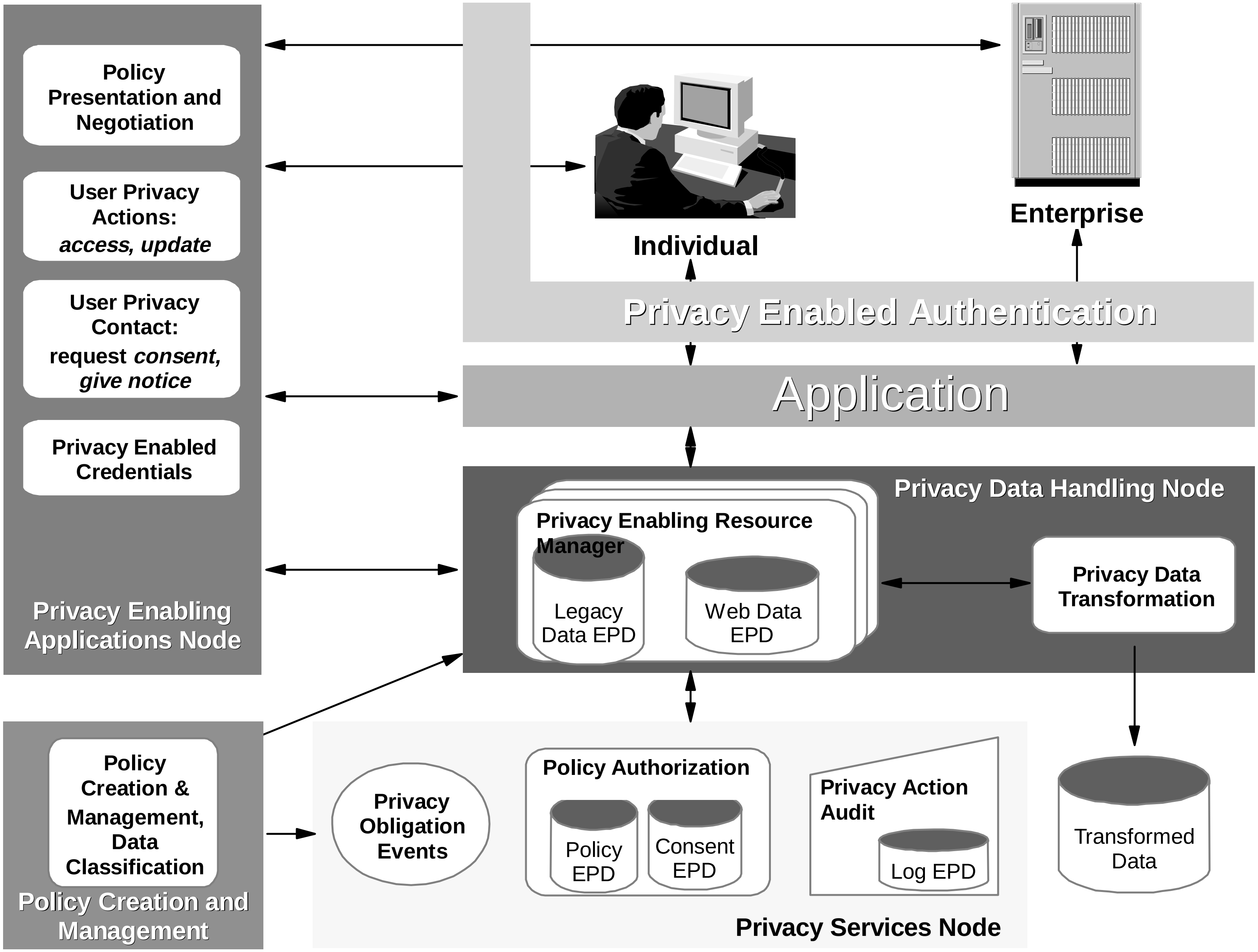
Subject
r Guardian
r Authority

give consent
update
access
withdraw consent

Data User

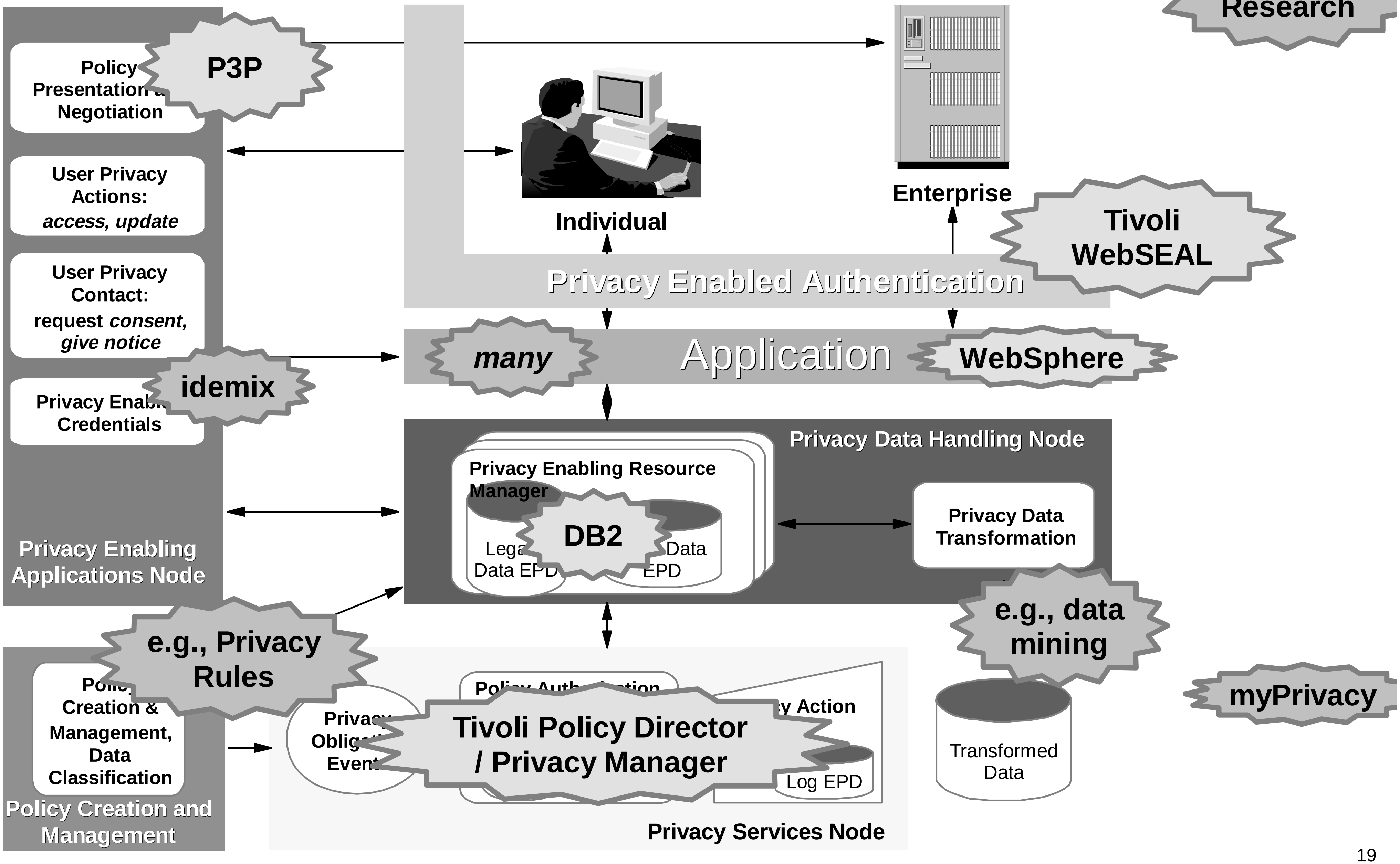
repersonalize
depersonalize

EPA - Technical Architecture


Policy Presentation and Negotiation
User Privacy Actions:
access, update
User Privacy Contact:
request *consent, give notice*
Privacy Enabled Credentials
Privacy Enabling Applications Node
Individual
Enterprise
Privacy Enabled Authentication
Application
Privacy Data Handling Node
Privacy Enabling Resource Manager
Legacy Data EPD
Web Data EPD
Privacy Data Transformation
Policy Creation & Management, Data Classification
Policy Creation and Management
Privacy Obligation Events
Policy Authorization
Policy EPD
Consent EPD
Privacy Action Audit
Log EPD
Transformed Data
Privacy Services Node

EPA - Technical Architecture

IBM Technology and Research


Policy Presentation a Negotiation
P3P
User Privacy Actions: *access, update*
User Privacy Contact: request *consent, give notice*
Privacy Enab Credentials
idemix
Privacy Enabling Applications Node
Individual
Enterprise
Tivoli WebSEAL
Privacy Enabled Authentication
many
Application
WebSphere
Privacy Data Handling Node
Privacy Enabling Resource Manager
DB2
Lega Data EPD
Data EPD
Privacy Data Transformation
e.g., data mining
Transformed Data
myPrivacy
e.g., Privacy Rules
Po Creation & Management, Data Classification
Policy Creation and Management
Privacy Oblig Event
Policy Auth
y Action
Tivoli Policy Director / Privacy Manager
Log EPD
Privacy Services Node

Privacy Manager

- Helps you *implement* your privacy policy
- *Reduces your risk* by controlling and auditing access to personally identifiable information
- Leverages and extends authorization services in Policy Director
- Features Include:
  - *Externalization of privacy management* from applications
  - *Fine-grained protection* enables you to place stricter rules on more sensitive data
  - *XML rules engine* enables context-based access decisions.
  - Pre-defined privacy data types, groups
  - *Sample Applications*
  - *"Instance-level" access control* and *dynamic roles* enhance the Policy Director Authorization capabilities.

Data-instance Level Authorization

- What if your authorization policy depends on the data being touched?
  - “To update psychotherapy notes, user must be the assigned mental health provider”
  - “To update the project due date, user must be the project manager of that project”

Healthcare Example

Policy: To update psychotherapy notes, user must be the mental health provider assigned to this patient.

Request: update_psych_notes on George

User: Anthony ☑

User: Tom ☒

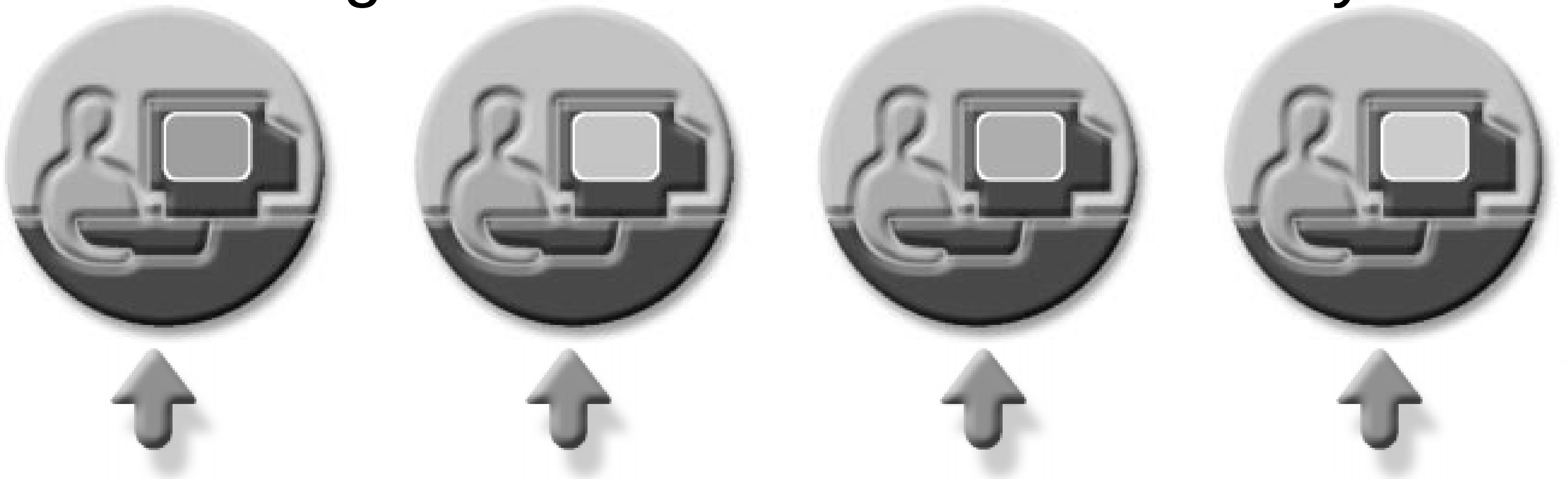
Patient	Assigned Mental Health Provider	Psychotherapy Notes
Dick	Tom	dsm1
George	Anthony	dsm2
Bill	Harriet	dsm3

Types of Access Control

- Policy Director controls access to applications
  - Access policies applied to users and groups
- Privacy Manager controls access to data
  - Access policies are context-based
  - Based on user's relationship to the data/request
  - Multiple conditions and factors may be considered by rules engine before access is granted

Managing Security Threats

No Integration = No Control = No Security



Firewall
Content Violations

IDS
Denial of Service Attacks

Access / Policy
Unauthorized Accesses

Web Server
CGI Vulnerabilities

Typical Implementation: Multiple Point Products

– Multiple sources of alarms / alerts
– Single problem can generate duplicity of events
– Inefficient operations due to multiple consoles
– Difficulty isolating critical / relevant problems

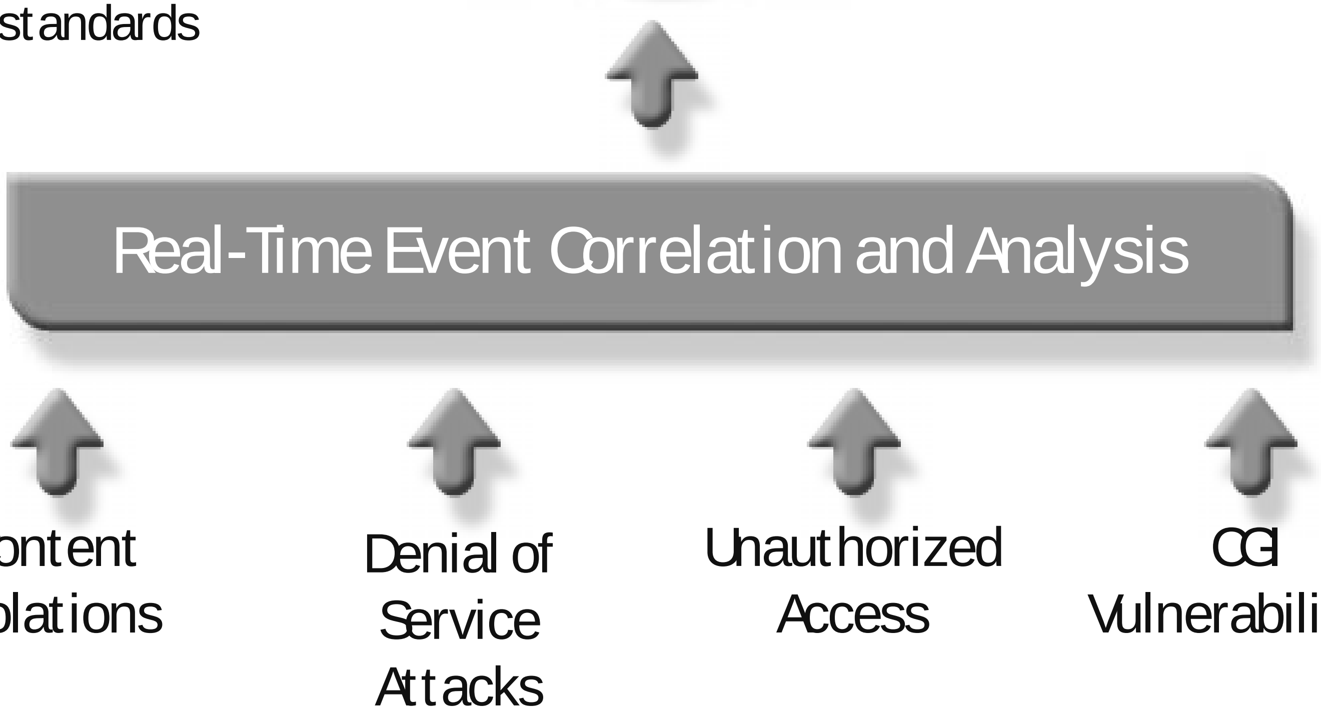
Solution: Integrated Risk Management

Exploiting the Power of Security:

- Centralized correlation
- Automated response
- Escalation of alerts
- Open standards

Successful Relationships:

- Eliminate false positives
- Single alert
- Role-based administration
- Consistent policy



Real-Time Event Correlation and Analysis

Content Violations

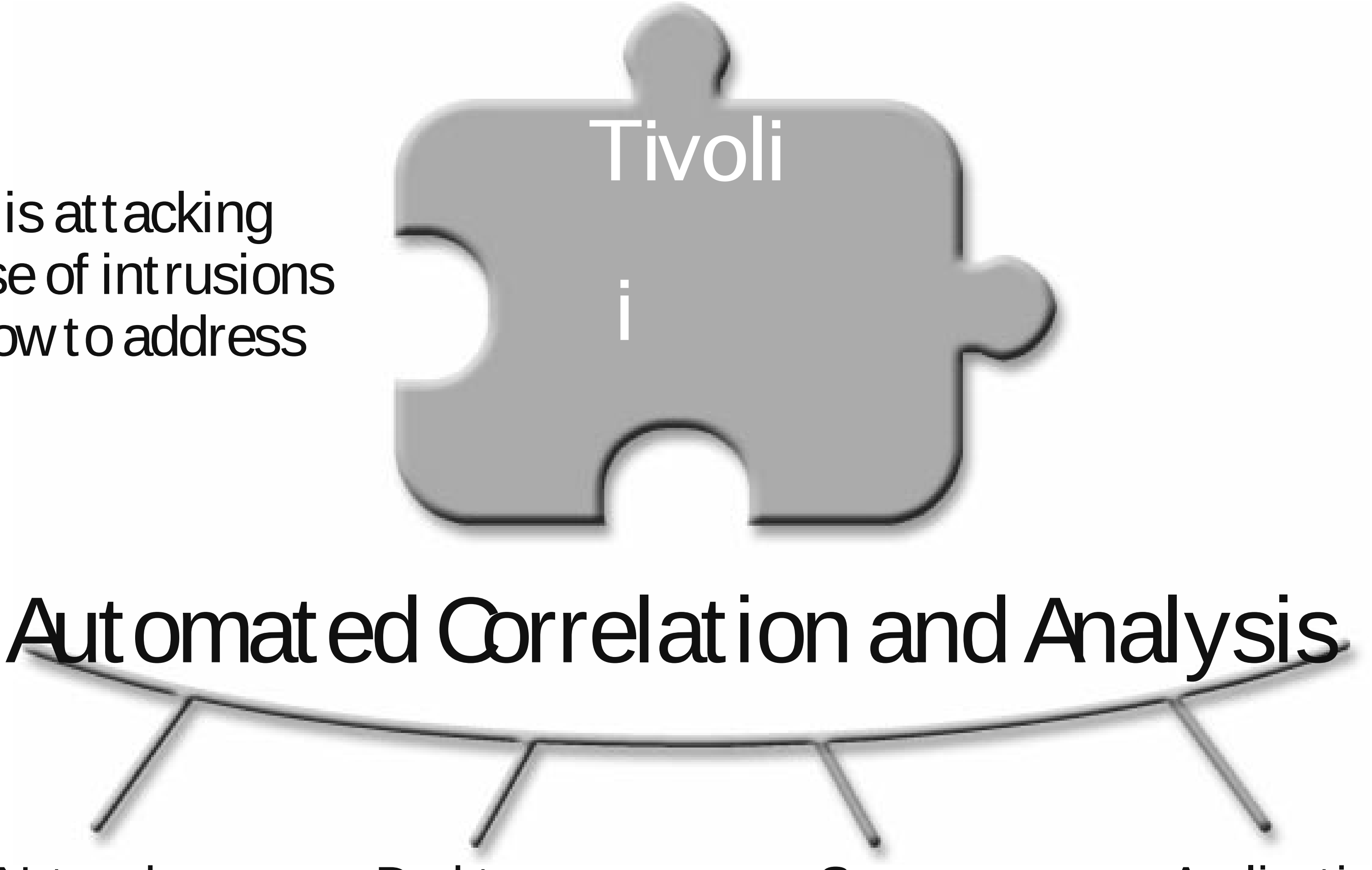
Denial of Service Attacks

Unauthorized Access

CGI Vulnerabilities

Tivoli SecureWay Risk Manager

- Identify who is attacking
- Analyze cause of intrusions
- Determine how to address threats



Tivoli

i

Automated Correlation and Analysis

Network Threats

Desktop Threats

Server Threats

Application Threats

Risk Manager Protects Against Security Threats

- Single control point to monitor, defend and respond to attacks and intrusions
- Faster, targeted response
- Reduce administrative costs: cross-product alert correlation, elimination of false positives
- Proactive Decision Support: empower the security analyst with intelligence, knowledge and Decision Support to respond to intrusions

z/OS SecureWay Security Server

- Intrusion Detection Services
- Kerberos support (NAS)
- PKI enhancements (CRL)
- LDAP enhancements
- SSL enhancements
- Aid in configuring VPNs
- Groups with unlimited # users
- Cryptographic services: SSL, UDE

Linux Security Requirements

- Hardware encryption
- Kerberos authentication
- LDAP and user management
- Firewall
- Public Key Infrastructure
- Policy Director
- Risk Manager
- Security management
- AntiVirus

Cryptography

- IBM Integrated Cryptographic Coprocessors
- IBM 4758 PCI Cryptographic Coprocessor
- IBM e-business Cryptographic Accelerator
  - PCI Secure Socket Layer (SSL) hardware accelerator adapter
  - offloads this compute-intensive public-key cryptographic processing from the host
  - RS/6000 and AIX 4.3.3+ or AIX 5L 5.1+
- PCD Embedded Security Chip
  - Trusted Computing Platform Specifications (TCPA)
  - Supports industry-standard cryptographic interface (MSCAPI and PKCS#11)
- Possible future algorithmic extensions:
  - AES - Rijndael?
  - Wireless - Elliptic Curve?

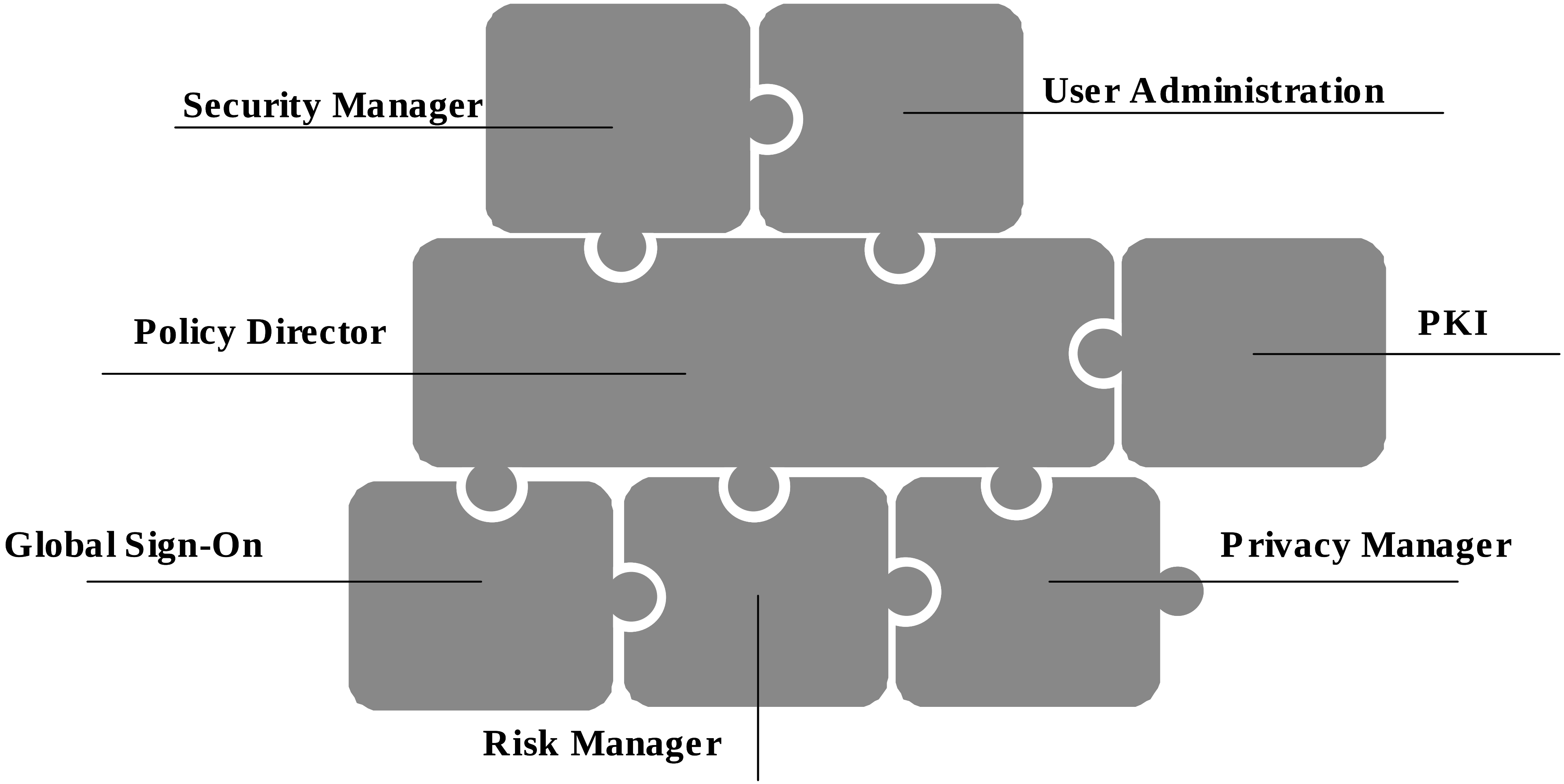
MISC Hot Topics

- Wireless Security
  - IBM joins alliance to fight cyber attacks(ITAA) (January 22, 2000)
  - Tivoli® SecureWay® Manages WAP Device Access to e-business Applications (June 6, 2000)
  - IDC Outlines Ideal Security Infrastructure for Wireless eBusiness (December 18, 2000)
  - IBM demonstrates first auditing tool for wireless network security (July 12, 2001)
- PKI and Identity Mapping
  - Tivoli® Drives Digital Signature Adoption in e-business (Tivoli SecureWay PKI for Identrus) (October 10, 2000)
  - New IBM Services Provide Foundation for Digital Signatures (November 8, 2000)
  - Entrust and IBM Make Mainframes Achieve Entrust-Ready Status (January 22, 2001)

References

- Tivoli SecureWay Policy Director
  - www.tivoli.com/products/index/secureway_policy_dir/
- Tivoli SecureWay Policy Director for MQSeries
  - www.tivoli.com/products/index/secureway_policy_dir_mqs/
- Tivoli SecureWay Privacy Manager
  - www.tivoli.com/products/index/secureway_privacy_mgr/
- Tivoli SecureWay Risk Manager
  - www.tivoli.com/products/index/secureway_risk_mgr/
- PCD Embedded Security Subsystem
  - www.pc.ibm.com/ww/security/securitychip.html
- IBM's Enterprise Privacy Architecture
  - www.ibm.com/services/security/epa.html
- z/OS SecureWay Security Server
  - www-1.ibm.com/servers/eserver/zseries/zos/security/securityserver.html
- Security research at IBM
  - www.research.ibm.com/compsci/security/
- IBM Security: www.ibm.com/security

Tivoli SecureWay


Security Manager
User Administration
Policy Director
PKI
Global Sign-On
Privacy Manager
Risk Manager