Enabling Trust in e-Business:
Research in Enterprise Privacy Technologies

Dr. Michael Waidner

IBM Zurich Research Lab

http://www.zurich.ibm.com / wmi@zurich.ibm.com

Outline

- Motivation
- Privacy-enhancing technologies
- Research in enterprise privacy technologies
- Summary

Outline

- **Motivation**
- Privacy-enhancing technologies
- Research in enterprise privacy technologies
- Summary

IBM Privacy Research Institute

" … As a result, consumers have become increasingly savvy about how businesses are using the information that they disclose on the Web. Seventy-five percent of consumers now report being wary of shopping online because of such disclosure fears, which is ***costing business roughly $15 billion annually****. … … The good news is* ***new technologies are coming*** *to market that give individuals the power to prohibit or limit others from tracking their movements on the Web. …"*

Steve Mills, August 2002

PRI's mission: To develop these new technologies, services and products, and to demonstrate thought leadership to our customers, partners and the scientific community.

People and businesses demand privacy technology

- People demand privacy
  - General concerns
    - 80-90% are concerned, 25% are fundamentalists
    - 6% think benefits from sharing PII online outweighed privacy concerns
  - General reservations
    - nobody gets a 5 on 1-7 trust scale for data like address and CC
  - Clear preferences
    - 91% demand 3rd-party audit of real privacy practices (not just of promises)
    - 90% demand security procedures, 84% access control, >80% enforced policies
  - Nothing changed after 9/11 towards enterprises

- Businesses expect
  - Increased e-business acceptance & privacy as differentiator
  - Reduced number of aborted transactions
  - Improved data quality

Outline

- Motivation
- **Privacy-enhancing technologies**
- Research in enterprise privacy technologies
- Summary

Privacy-enhancing technologies

Privacy-enabling Infrastructure

Client

- Trusted user device?
- Identity management
  - Pseudonyms, preferences, negotiation
  - User interface
- Filtering and privacy violation detection
- Customization

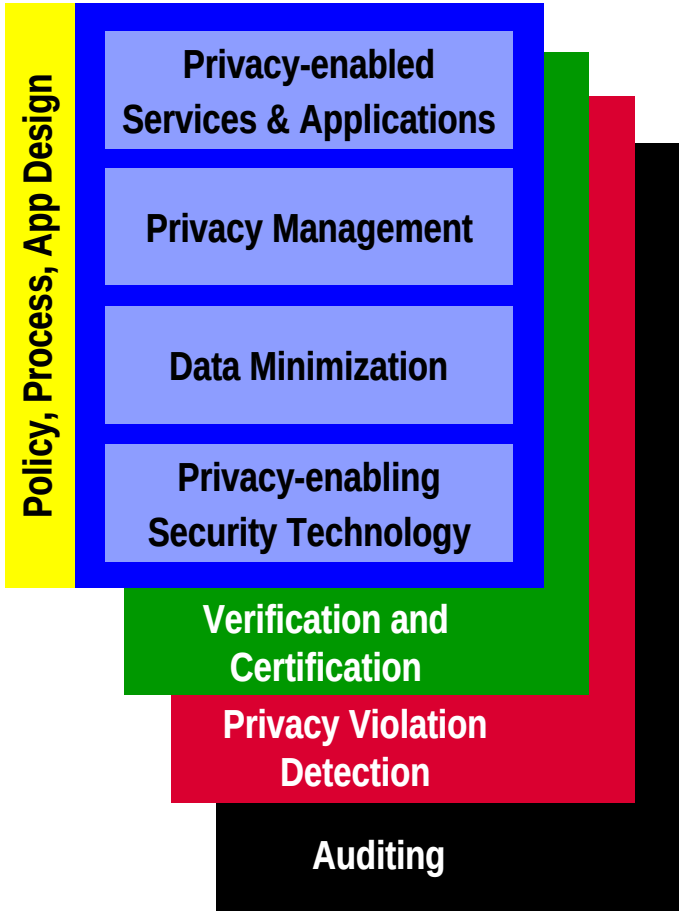
- Communication
- Trust
  - Certified attributes
  - Authentication
  - Identity
- Payment and delivery
- Convenience
  - SSO
  - Attributes

Organization

- Exploration of status quo
- Process (re-)engineering
  - Data minimization paradigm
- Policy
  - Creation, translation, consistency, versioning
  - Authorization and enforcement
- Identity/profile mgmt
- Customer privacy services
- Privacy violation detection
- Auditing

Privacy-enhancing technologies

- Technology
  - Helps to agree on fair privacy policies, to enforce them, and to manage privacy.
  - Helps to minimize the personal information released/disclosed, or used by a process.
  - Helps to keep honest people honest, and protects personal information.
  - Helps to build trust and customer loyalty.



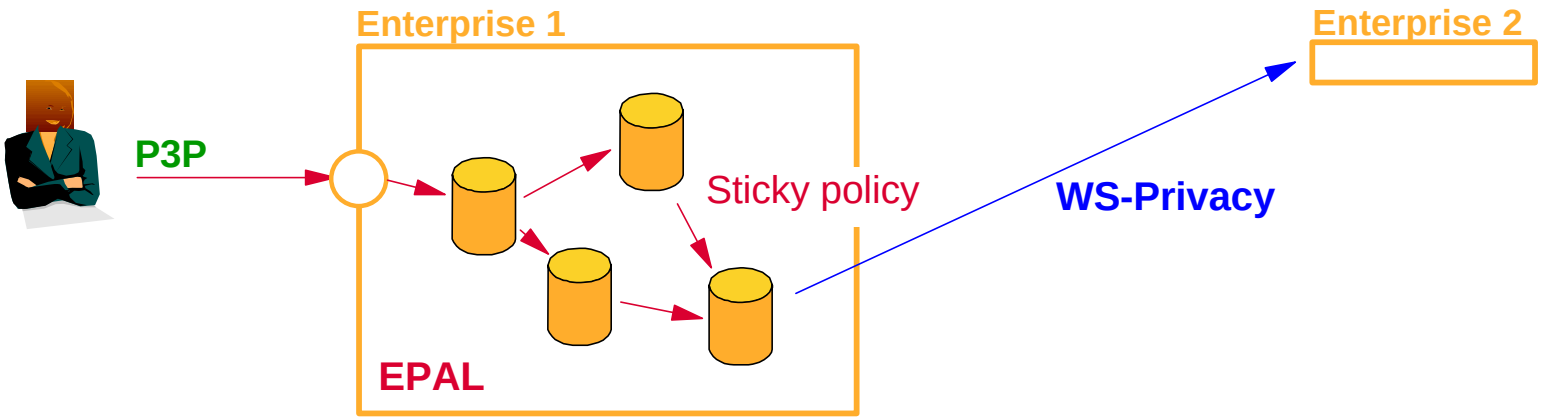
Outline

- Motivation
- Privacy-enhancing technologies
- **Research in enterprise privacy technologies**
- Summary

1. Enterprise privacy management

- **Enterprises want better privacy for their customers – but need support.**
  - **Formalizing a privacy policy**
    - Machine readable, addresses internal procedures, going beyond P3P
  - **Deploying the privacy policy**
    - Get abstract privacy policy connected to real data (DB2, files, …)
  - **Recording consent**
    - Offer opt-in and opt-out, be prepared for “access”
  - **Enforcing/auditing privacy**
    - Ensure that nobody gets access who is not entitled for it
  - **Reporting & privacy services**
    - Which privacy violations occurred?
    - What data is stored about Mary Smith?
  - **Help developers to get it right …**
    - Get privacy policies into the business processes
    - Application and process development tools become privacy-aware

EPAL Enterprise privacy policies

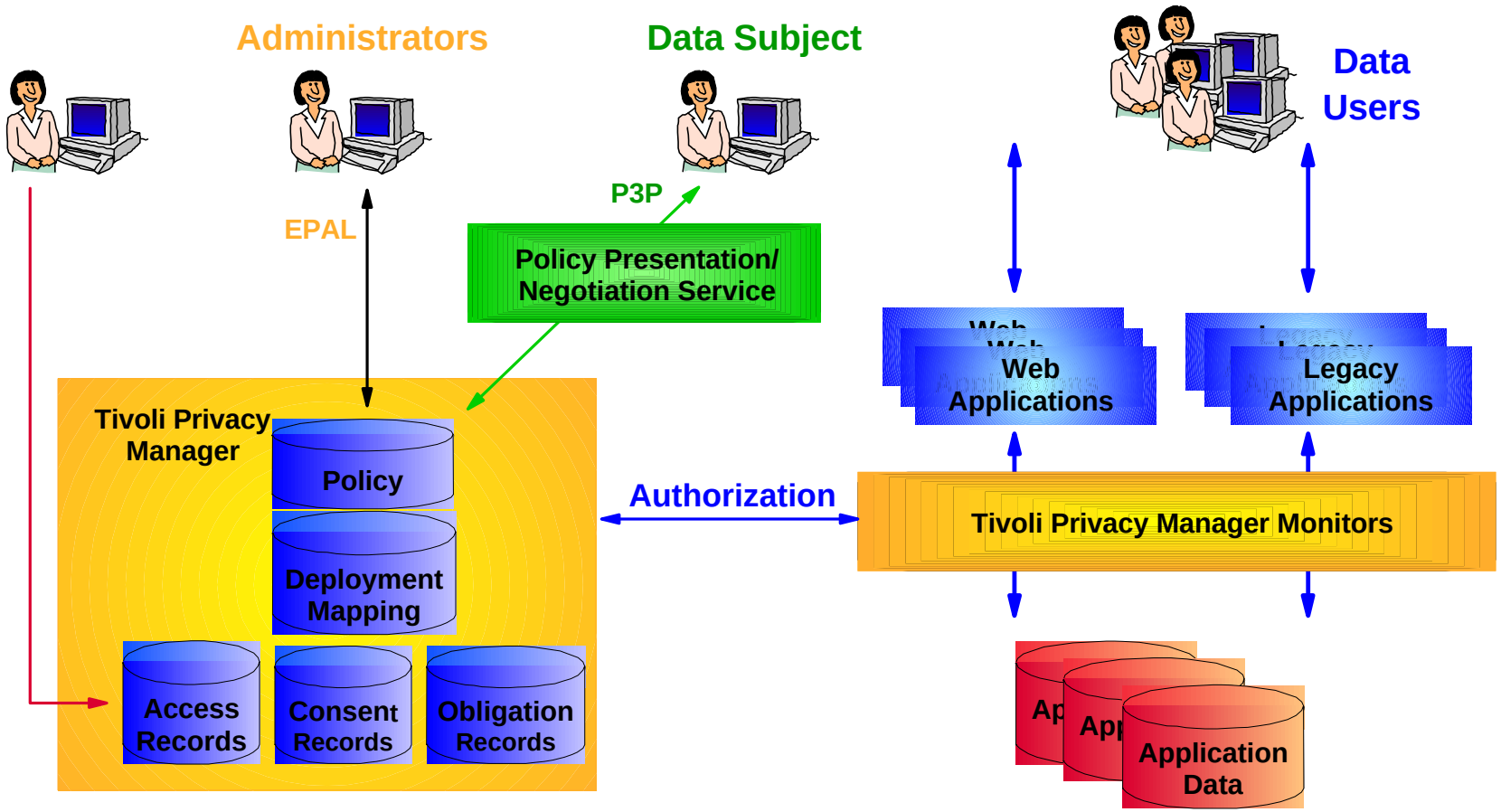


- Rules use "if-then-else" logic:
  - A privacy relevant operation is permitted, if ...
- Policy refines promises with enterprise-internals:
  - Only a simplified version is displayed to the customer (e.g., as P3P policy)

Example syntax

- EPAL rules authorize access:
  - "Operation by data user on data category, for purpose under condition resulting in obligation"
- EPAL definitions define scope:
  - Data users, purposes, categories as hierarchies
  - Operations, obligations as lists
- *"Email can be used for the book-of-the-month club if consent has been given and age is more than 13"*
  - <ALLOW
    data-user="borderless-books"
    data-category="email"
    purpose="book-of-the-month-club"
    operation="read"
    condition= "/CustomerRecord/Consent/BookClub=True &&
    /CustomerRecord/age>13">

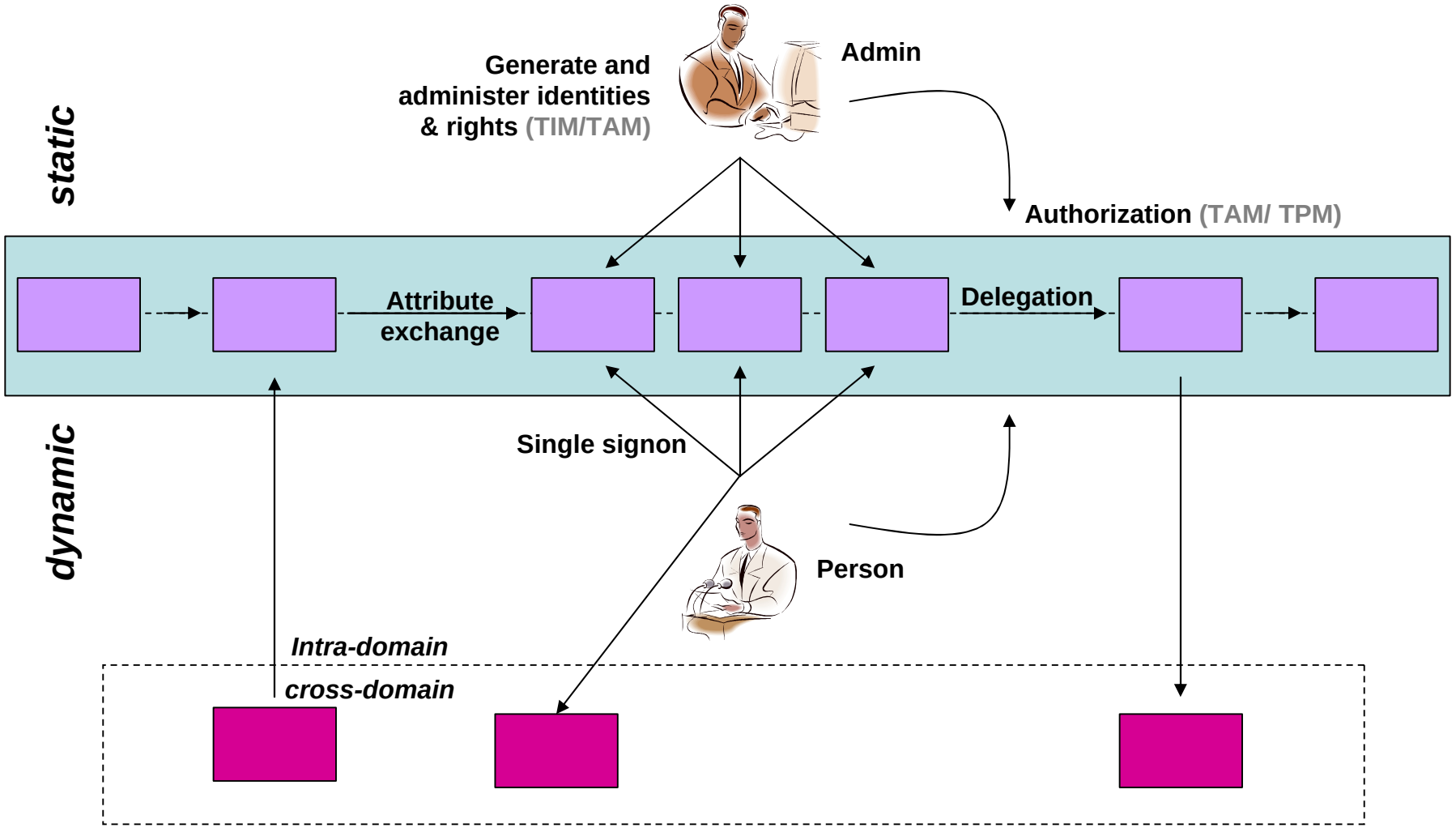
Privacy management architecture



2. Integrated security, identity, privacy (SIP) management

- **Products and infrastructure for managing Security, Identity, and Privacy will converge into integrated, interoperable products.**
  - Take advantage of synergies to reduce costs and support customer-centric business models
  - Decrease complexity and reduce misconfigurations and mismanagement.
  - Federations preserving security & privacy across trust domains will be enabled through well-defined, contract-based Web services.

Identity and privacy management



Identity and privacy management

- Architectures for security, identity and privacy management
  - Integrated data models, user and authorization models
  - Standard interfaces, languages and protocols
- Privacy-friendly protocols for single signon, attribute exchange, and delegation
- Combine pseudonymity and server-side SIP management
  - Pseudonymous and attribute-based authorization

3. Critical applications will be addressed by new solutions

- **Public-key infrastructures**
  - Novel crypto tricks will give individuals full control over information included in attribute certificates
- **Statistical data mining**
  - Novel randomization tricks let enterprises make statistics w/o putting individual records at risk.
- **Surveillance technologies**
  - Novel image processing technologies will hide all personally identifiable info, until needed (if ever)
- **Pervasive computing**
  - Novel privacy management tools help individuals to understand and set their personal policies.
  - Even intelligent dust will have a privacy policy.

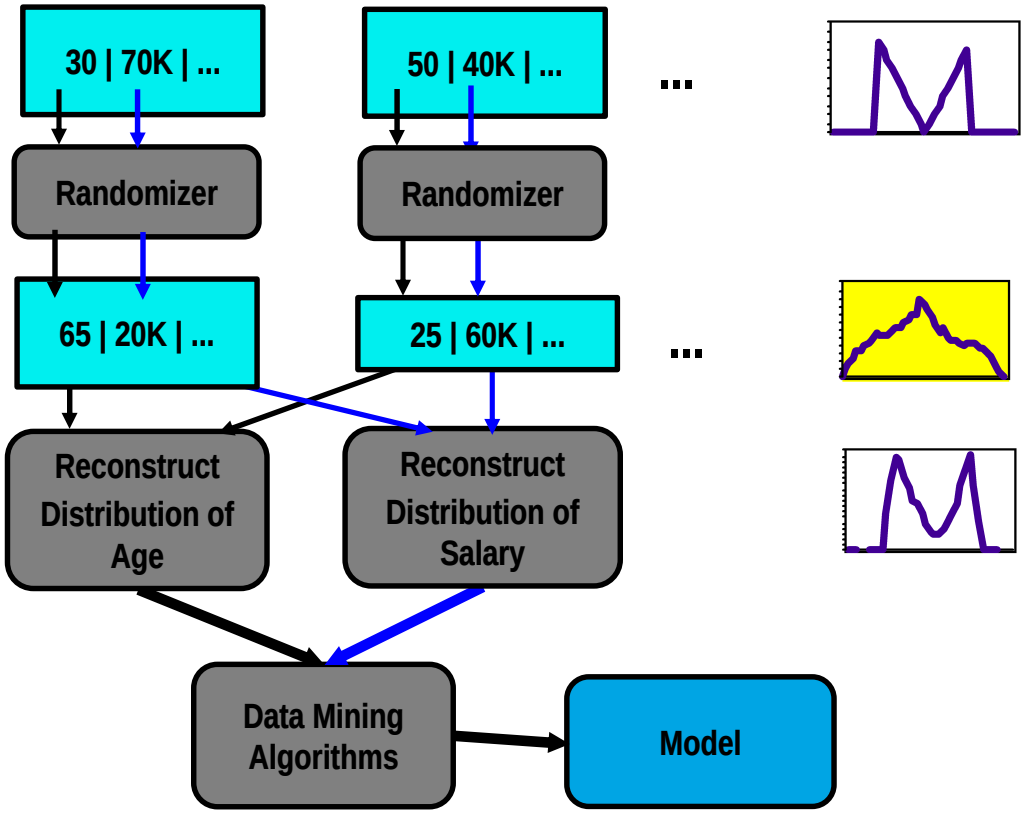
Public-key infrastructures: idemix Approach

- Step 1: Pseudonyms
  - Organizations know individuals by pseudonyms only
- Step 2: Control attributes
  - Only necessary attributes are shown
- Step 3: Standardize attributes
  - Effective only if shown attributes don't identify individuals (rather an application requirement ...)
- Step 4: Prove knowledge of cert's
  - Certificates are kept secret, only their possession is shown (zero-knowledge proofs of knowledge)

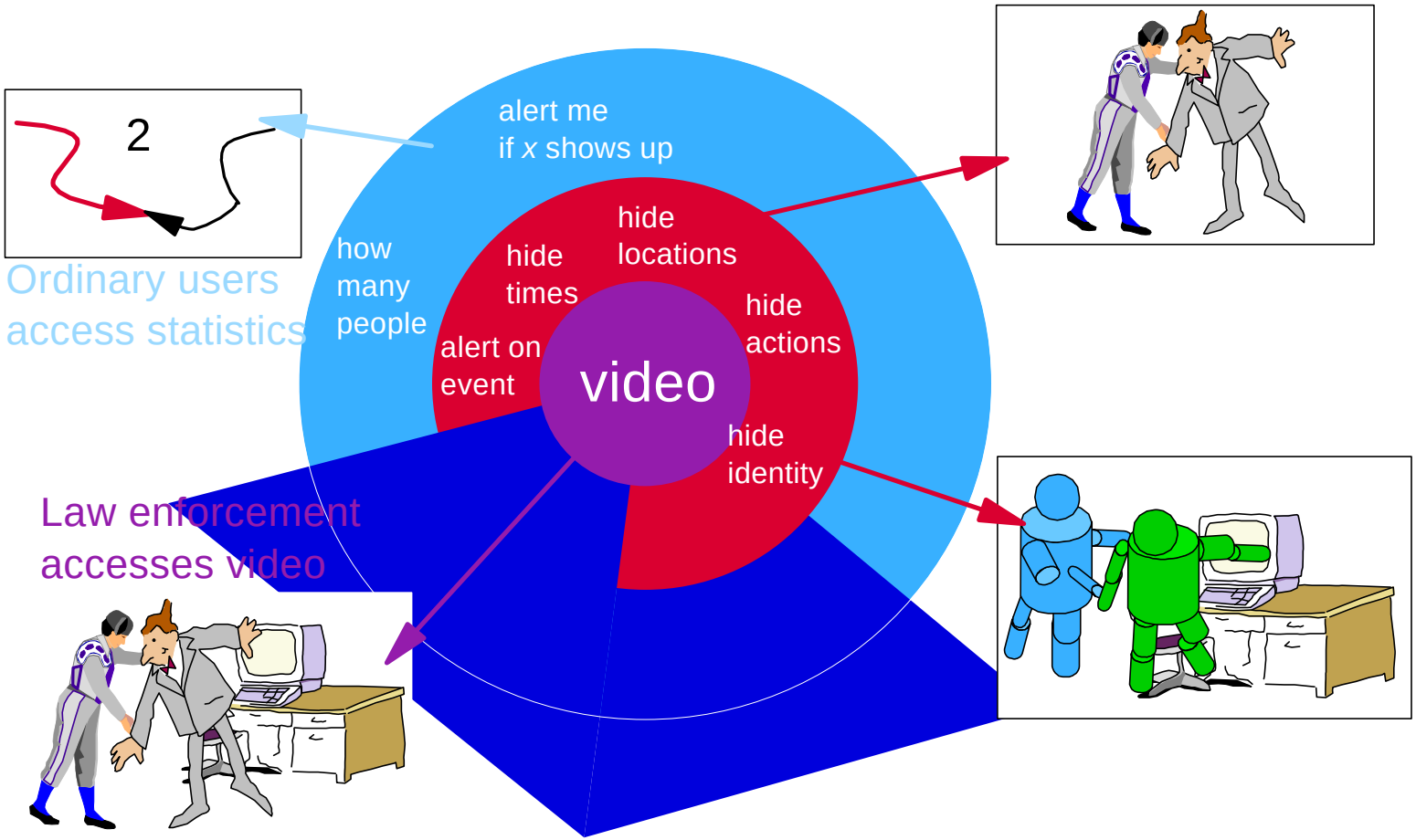
Public-key infrastructures: status & scenarios

- Status
  - Achieves maximum (!) of privacy in PKI-based transactions
  - Depends on advanced crypto algorithms
    - Provably secure
    - Efficient and practical
- Application scenarios
  - Anonymous electronic transactions
  - Anonymous subscriptions
  - Anonymous access to pervasive infrastructure

Statistical data mining: privacy preserving data mining



Surveillance technologies: privacy enhancing cameras



Outline

- Motivation
- Privacy-enhancing technologies
- Research in enterprise privacy technologies
- **Summary**

IBM Privacy Research Institute

- Our mission
  - To develop new enterprise privacy technologies, services and products, and to demonstrate thought leadership to our customers, partners and the scientific community
- Why?
  - Privacy is more than a cerebral debate – it's a business issue
  - Customers and employees must trust that we keep their personal information secure and private
  - E-business will continue to evolve with that trust
- How?
  - More than 40 scientists at the 8 IBM Research labs
  - Close cooperation with teams at IBM Tivoli and IBM Global Services
  - Marketplace realities and needs are at the fore of our thought and solutions

IBM Privacy Research Institute

- Research priorities
  - Enterprise privacy management
    - Models and architectures
    - Languages and enforcement architectures
    - Tools
  - Integrated security, identity, privacy (SIP) management
    - Privacy-friendly identity management
  - Critical applications will be addressed by new solutions
    - Pseudonymity & public-key infrastructures
    - Statistical data mining
    - Surveillance technologies
    - Pervasive computing

For more information …

- How to reach me
  - Michael Waidner <wmi@zurich.ibm.com>
  - http://www.zurich.ibm.com/~wmi
- IBM Research
  - IBM Research: http://www.research.ibm.com
  - IBM Privacy Research Institute: http://www.research.ibm.com/privacy
- Privacy at IBM
  - http://www.ibm.com/security/privacy