Identity Management: Enterprise, E-Commerce and Government applications and their implications for privacy

Joe Pato, Principal Scientist
Trust, Security & Privacy
HP Labs

Guest Lecture - CPSC 155b
10 April 2003

Introduction

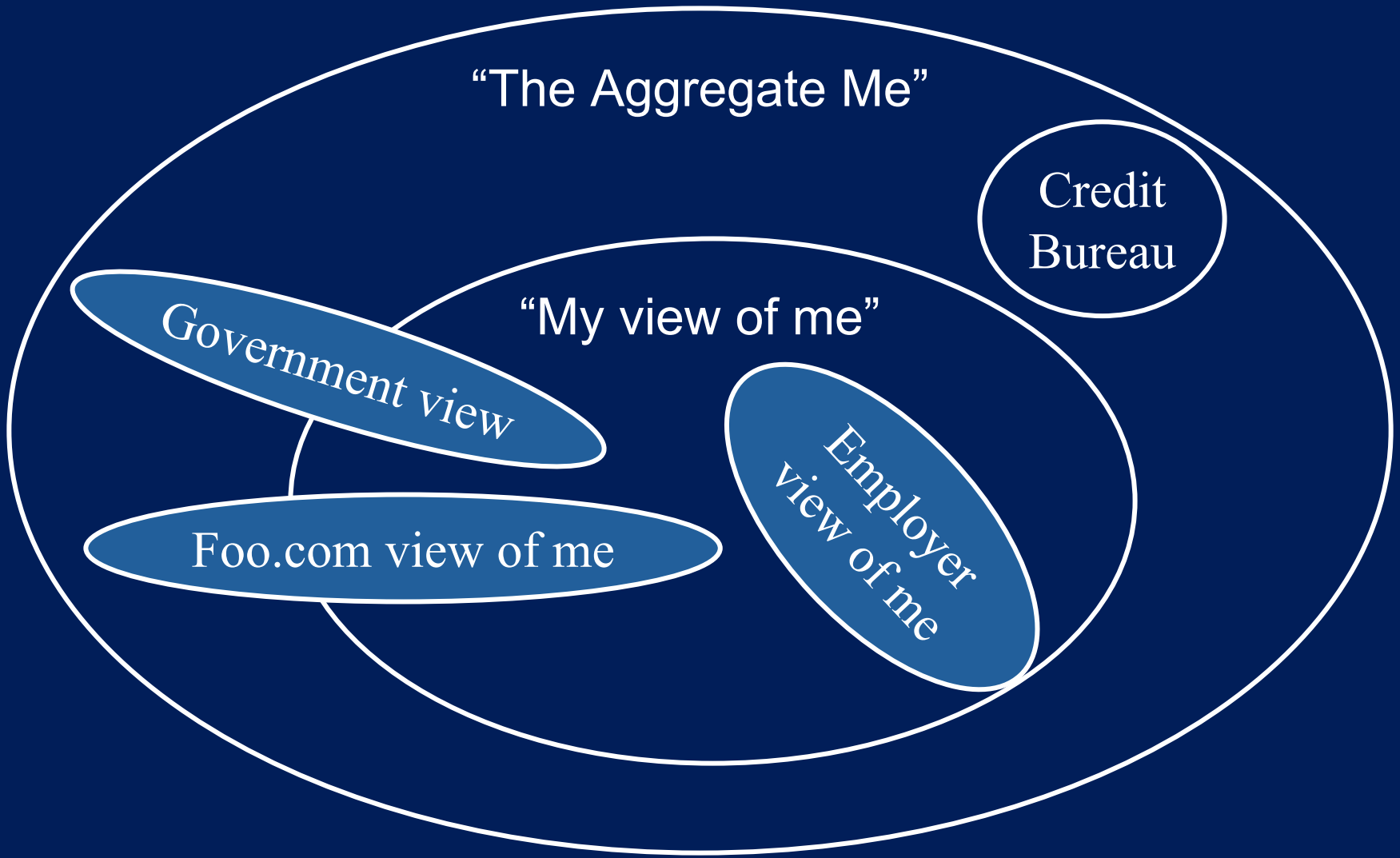
- Future – Ubiquitous Computing
  - Ginger Segue
- Identity Management
  - What is Identity
  - Authentication
  - Enterprise / Internet / Government contexts
- Privacy Considerations

Identity Management

Identity Management is:

- the set of processes, tools and social contracts surrounding
  - the creation
  - maintenance
  - and termination of a digital identity
- for people or, more generally, for systems and services
- to enable secure access to an expanding set of systems and applications.

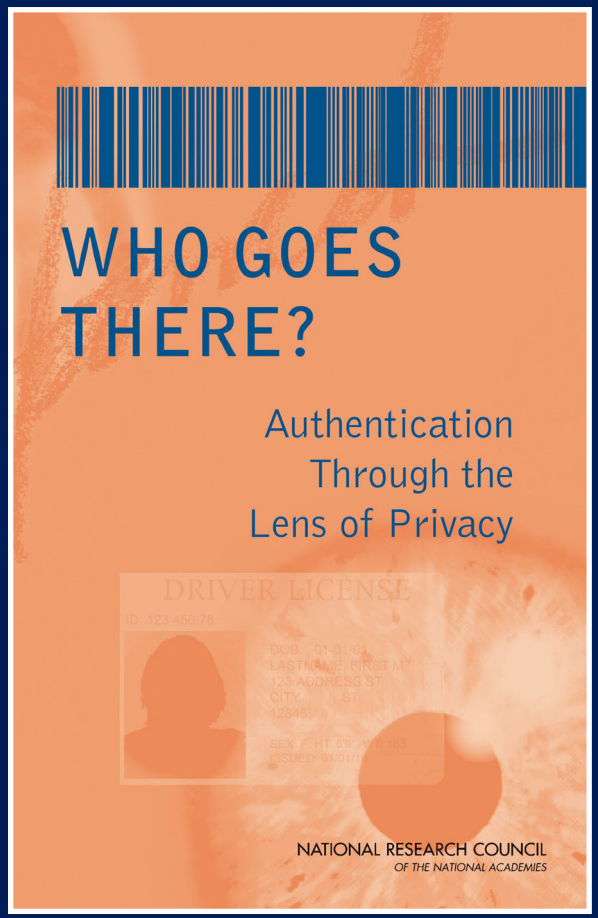
Views of Identity



Some Definitions

CSTB • Computer Science and Telecommunications Board

- Courtesy of



Who Goes There? Authentication Through the Lens of Privacy

Committee on Authentication Technologies and Their Privacy Implications

Computer Science and Telecommunications Board
The National Academies
Washington, D.C.
http://cstb.org/

Individual

An individual is a person.

Identifier

CSTB · Computer Science and Telecommunications Board

"Lamont Cranston"

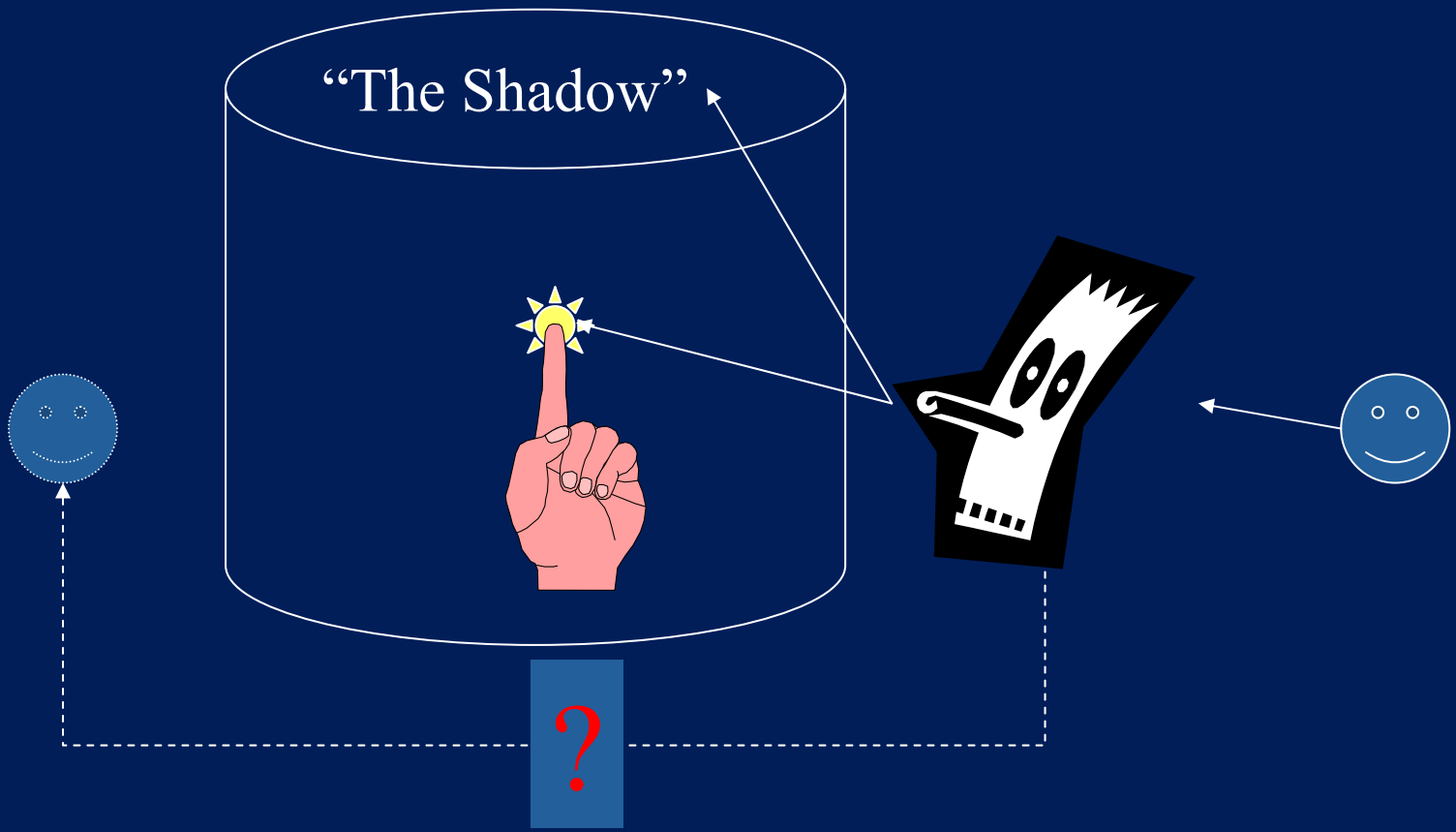
"Employee #512657"

An identifier identifies an individual.

Attribute

An Attribute describes a property associated with an individual

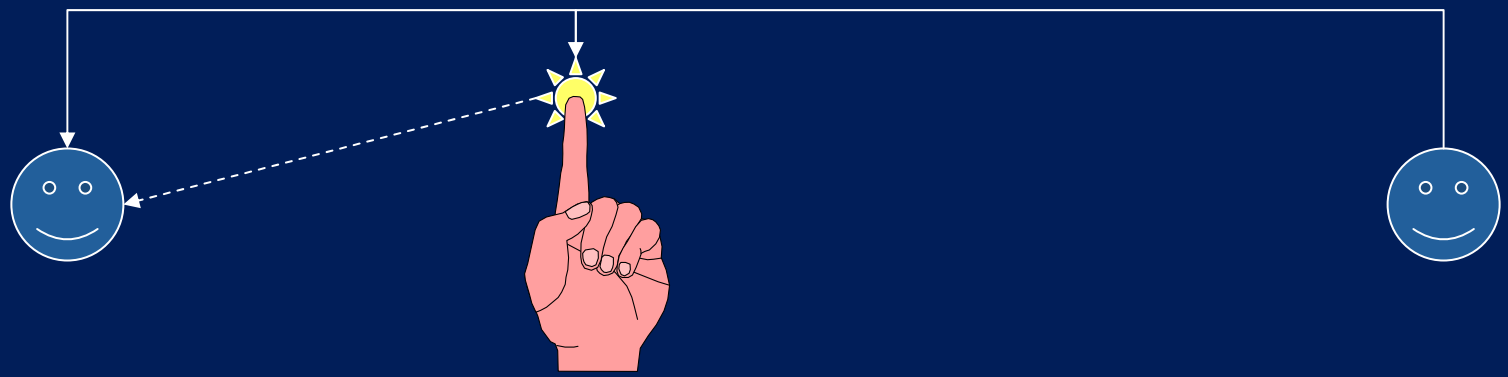
Identity



"an identity of X" is the set of information about an individual X associated with that individual in a particular identity system Y

CSTB · Computer Science and Telecommunications Board

Identification



Identification is the process of using
claimed or observed attributes of an individual
to infer **who** the individual is

Authenticator

CSTB • Computer Science and Telecommunications Board

An authenticator is evidence which is presented
to support authentication of a claim.
It increases confidence in the truth of the claim

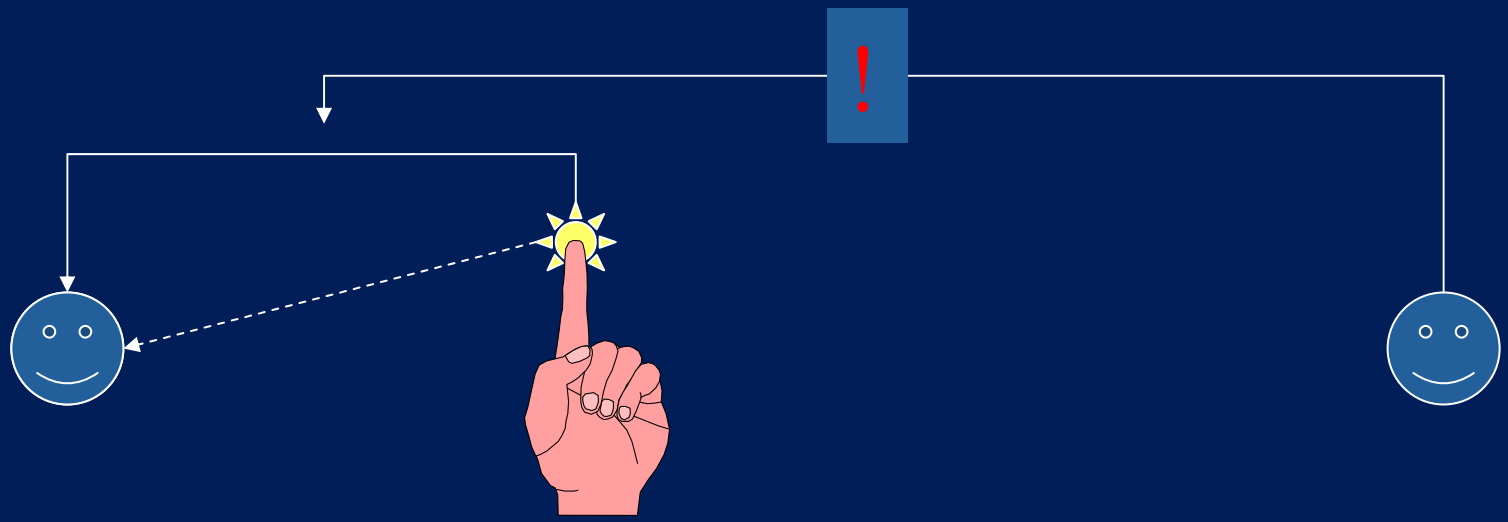
Authentication

CSTB · Computer Science and Telecommunications Board

Authentication is the process of establishing confidence in the truth of **some claim**

There are different types of authentication…

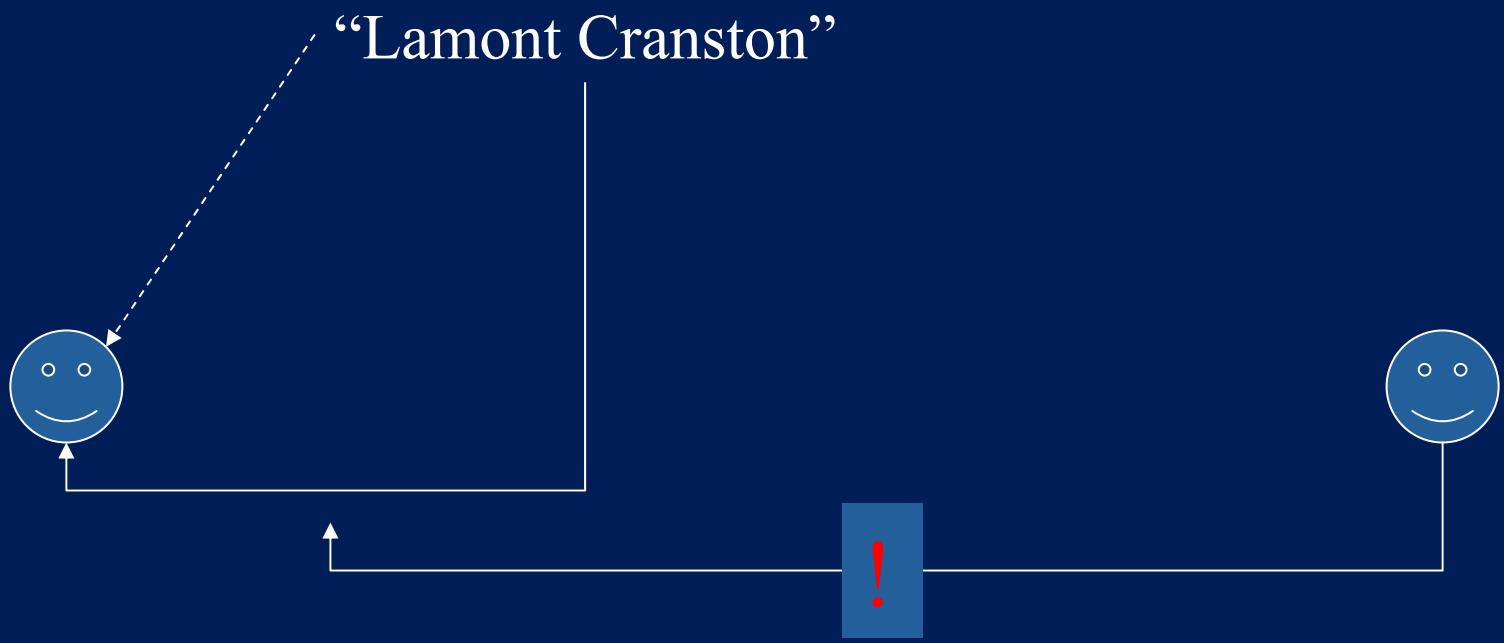
Attribute Authentication



Attribute Authentication is the process of establishing
an understood level of confidence
that an attribute applies to a specific individual

CSTB · Computer Science and Telecommunications Board

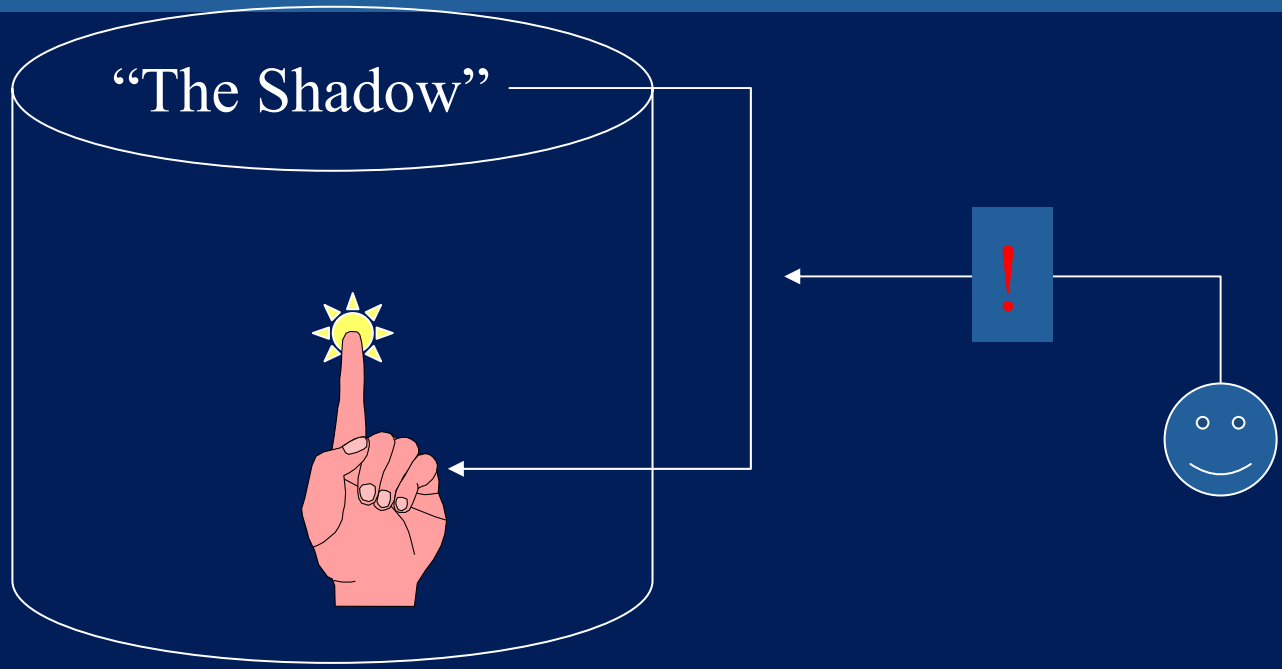
Individual Authentication



Individual Authentication is the process of establishing an understood level of confidence that an identifier refers to a specific individual

CSTB · Computer Science and Telecommunications Board

Identity Authentication



Identity Authentication is the process of establishing
an understood level of confidence
that an identifier refers to an identity

CSTB · Computer Science and Telecommunications Board

Authorization

CSTB · Computer Science and Telecommunications Board

Authorization is the process of deciding
what an individual ought to be allowed to do

Internet vs. Enterprise

- Organizational control of population
- Ability to issue tokens
- Ability to mandate desktop software
- Direct vs. network access
- Scale of population
- Privacy Issues

Government's Unique Role

- Regulator, Issuer of identity documents, Relying Party
- Unique Relationship with Citizens
  - Many transactions are mandatory
  - Agencies cannot choose their markets
  - Relationships can be cradle-to-grave
  - Individuals may have higher expectations for government
- Provider of Services
  - A common identifier may be in tension with principles of Privacy Act

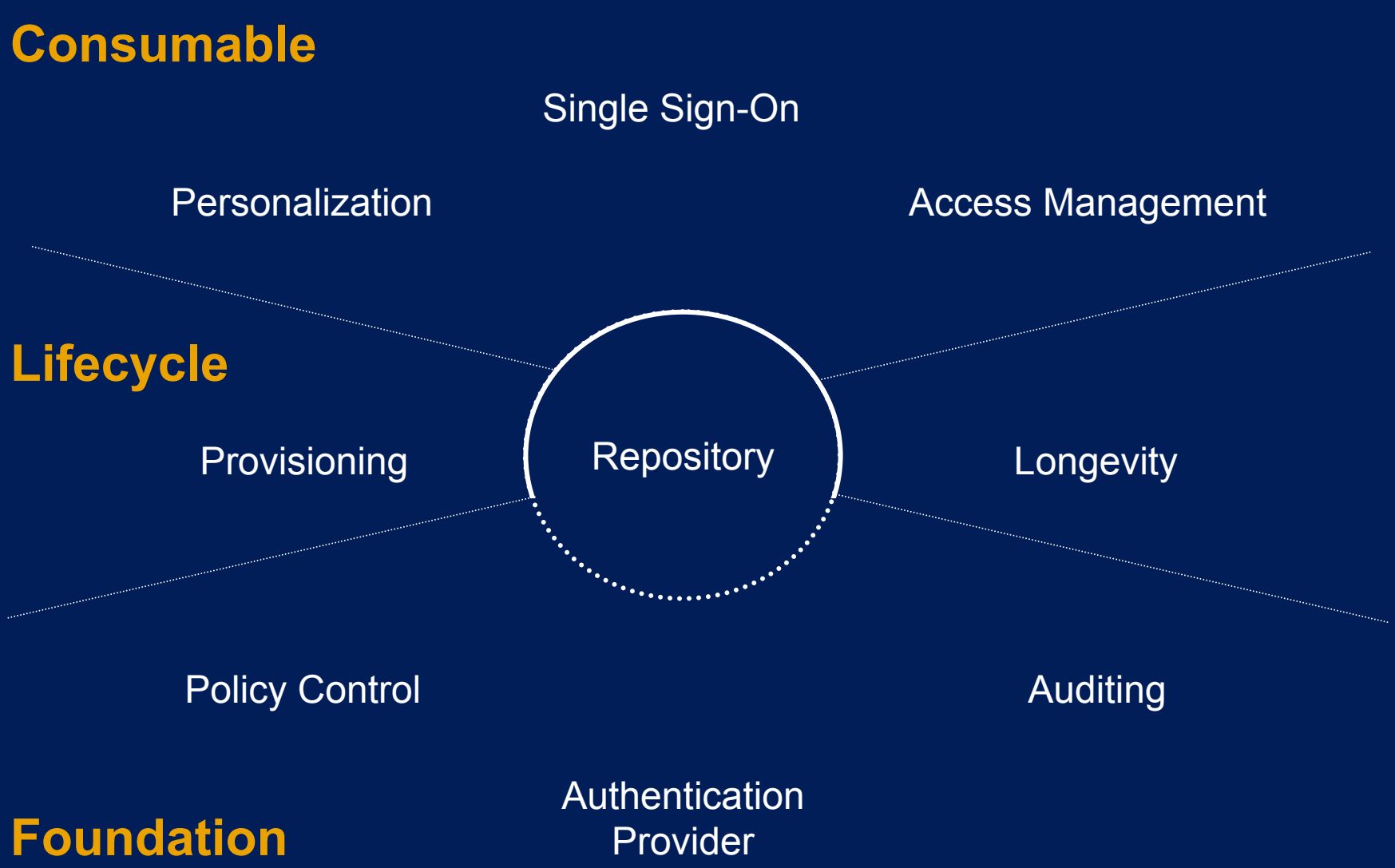
CSTB • Computer Science and Telecommunications Board

Foundational Documents Pose Risks

- Many of these documents are very poor from a security perspective
  - Diverse issuers
  - No ongoing interest on part of issuer to ensure validity/reliability
- Birth certificates are particularly poor
  - Should not be sole base identity document

CSTB • Computer Science and Telecommunications Board

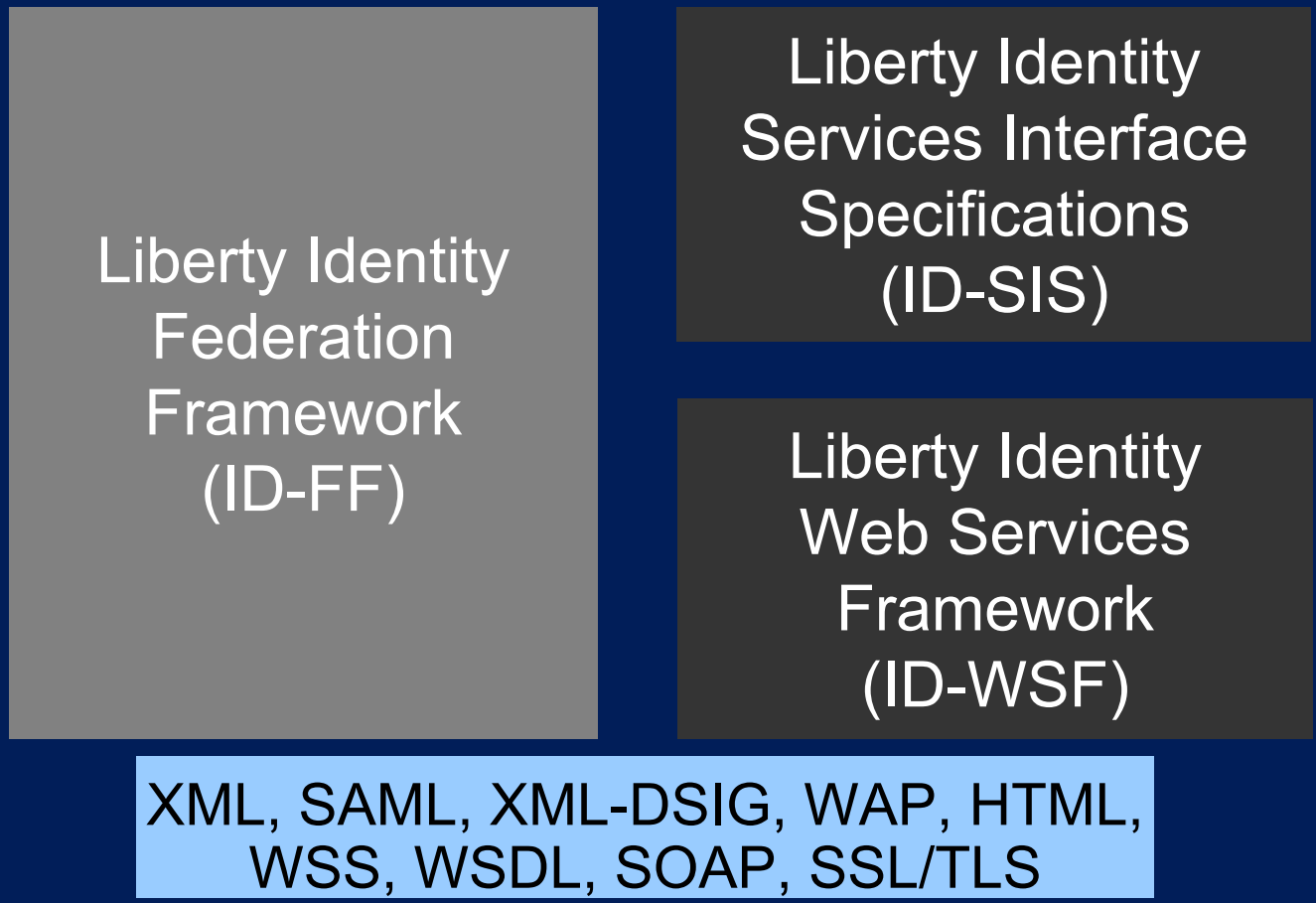
Identity Management Components



Authentication Technologies

- Passwords
- Tokens
- Smartcards
- Biometrics
- PKI
- Kerberos

Federated Identity: Liberty Alliance



Privacy

- Numerous philosophical approaches
- Four types discussed here
  - Information privacy
  - Bodily integrity
  - Decisional privacy
  - Communications privacy

CSTB • Computer Science and Telecommunications Board

General Privacy Implications

- Authentication can implicate privacy – the broader the scope, the greater the potential privacy impact
- Using a small number of identifiers across systems facilitates linkage, affects privacy
- Incentives to protect privacy are needed
- Minimize linkage and secondary use

CSTB • Computer Science and Telecommunications Board

Multiple Stages at which Privacy is Affected

CSTB • Computer Science and Telecommunications Board

- Authentication, generally
- Choice of Attribute
- Selection of Identifier
- Selection of Identity
- The Act of Authentication
- These are just in the design stage, before transactional data collection, linkage, secondary use issues, etc.
- Chapter 7's toolkit describes each of these in detail

1. Authentication's Implications Separate from Technology:

CSTB • Computer Science and Telecommunications Board

- The act of authentication affects privacy, regardless of the technology used
- Requires some revelation and confirmation of personal information
  - Establishing an identifier or attribute
  - Potential transactional records
  - Possible exposure of information to parties not involved in authentication

2. Attribute Choice Affects Privacy

CSTB • Computer Science and Telecommunications Board

- Informational privacy
  - Distinctive vs. more general
  - Minimize disclosure
  - Ensure data quality
  - Avoid widely-used attributes
- Decisional – If sensitive, may impinge willingness
- Bodily integrity – If requires physical collection, may be invasive
- Communications – If attribute reveals address, phone, network

3. Identifier Selection Affects Privacy

- Informational privacy
  - Identifier itself may be revealing
  - Will link to the individual
- Decisional – Fewer effects if random or if allows for pseudonymous participation
- Bodily integrity – Minimal effects
- Communications – Problem if identifier is address or number (telephone, IP address, etc.)

4. Identity Selection Affects Privacy

- Three possibilities
  - Identifier is only information available to the system
  - Identifier is not linked to information outside of the system
  - Identifier may be linked to outside records
- Tracking transactional information poses risk to decisional privacy
- All issues related to identifier choice remain relevant here

5. Act of Authentication Affects Privacy

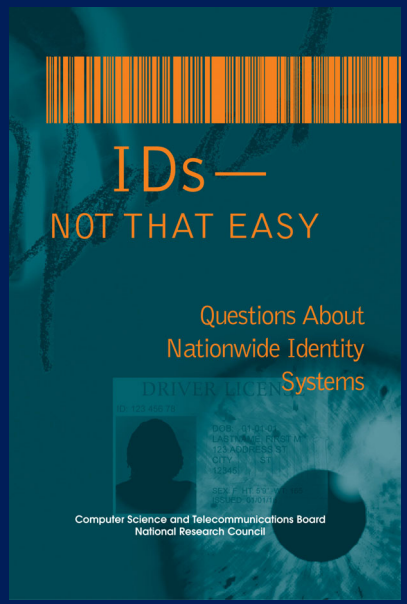
- Authentication usually accomplished by observing the user or requiring support of the claim
- Informational – If records are kept
- Decisional – Intrusiveness and visibility may affect
- Bodily Integrity – If close contact is required
- Communications – If communication systems use is required

Additional Issues

CSTB • Computer Science and Telecommunications Board

- When is authentication really necessary?
- Secondary use of identifiers
  - Without original system limits in mind, usage can become highly inappropriate
  - This can lead to privacy and security problems, compromise original mission, and generate additional costs
- Explicit recognition of the appropriateness of multiple identities for individuals
- Usability
  - Design systems with human limits in mind!
  - Employ user-centered design methods
- Identity theft as a side effect of authentication system design choices

As for Nationwide Identity Systems…



- Driver's licenses are a nationwide identity system
- The challenges are enormous
  - Inappropriate linkages and secondary use likely without restrictions

- Biometrics databases and samples would need strong protection
- Any new proposals should be subject to analysis here and in *IDs—Not That Easy*

Questions

???

Follow-up:

Joe Pato

HP Labs

One Cambridge Center – 11’th Floor

Cambridge, MA 02142

joe.pato@hp.com