Identity Management Standards

For Product Life Cycle of Electronic Parts

Ya-Shian Li-Baboud
Eric Simmon
Yaw Obeng

ya-shian.li-baboud@nist.gov

NIST

Outline

- Challenges
- Identity Management
- Standards
- Other Industries
- Pitfalls and Lessons Learned
- Opportunities

Challenges

Counterfeit detection

- Identical appearance for packaging and product
- Requires expertise, forensics

Data accessibility, synchronization and quality

- Enforcement officers require access to identity data
- Fragmented databases and workflows

Cost

- Managing risk-cost tradeoffs

Dynamic nature

- Cat and mouse game

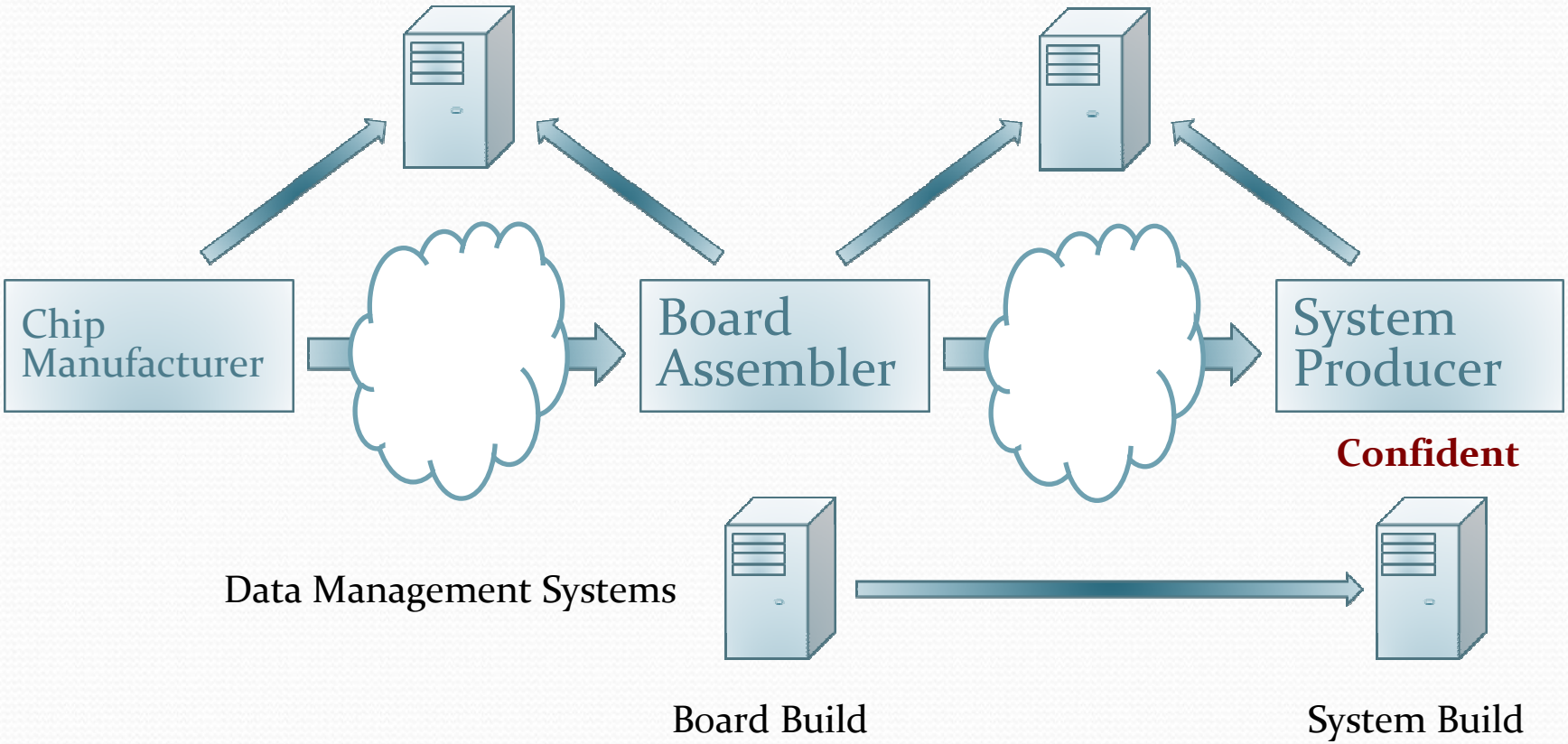
Confidentiality and privacy

- Sellers and buyers

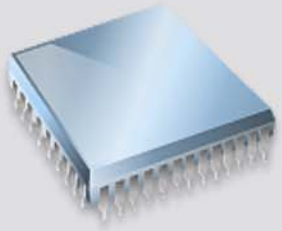
Assessing security

- Is the identity management solution secure?

Supply Chain (sub)Product



Product Lifecycle



Concept & Design

- Fabless
- Design foundries
- IDM

Manufacture

- IDM
- Foundries

Assembly & Test

- Packaging
- Assembly
- Test

Distribute & Support

- Buyers/Distributors
- Electronic Manufacturing Services
- OEMs

Disassemble & Recycle

- E-Waste
- Reuse
- Local Government Recycling Centers
- EPR

Identity Management

Product Authentication

Identity Management

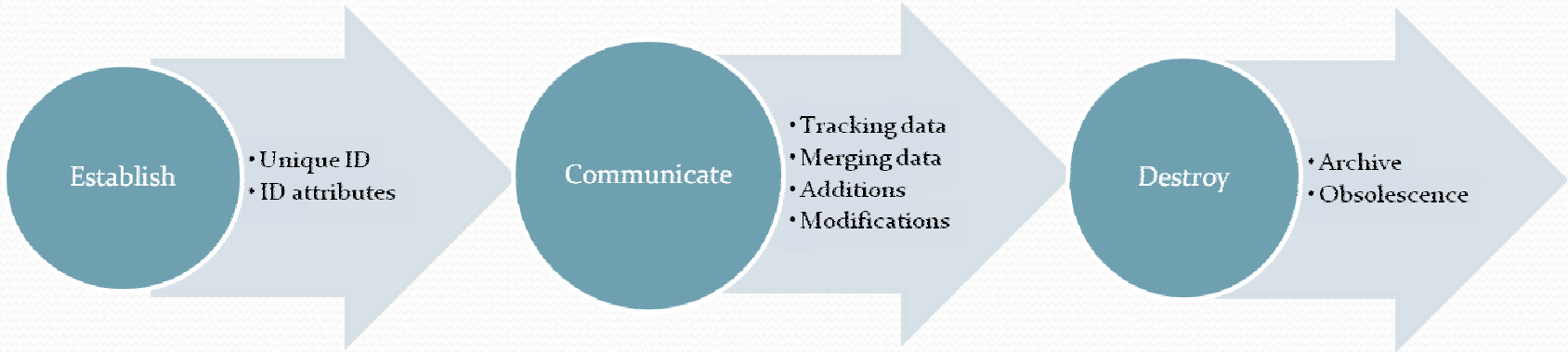
Managing the Identity of the Product

- Authentication
- Tracking
- Traceability

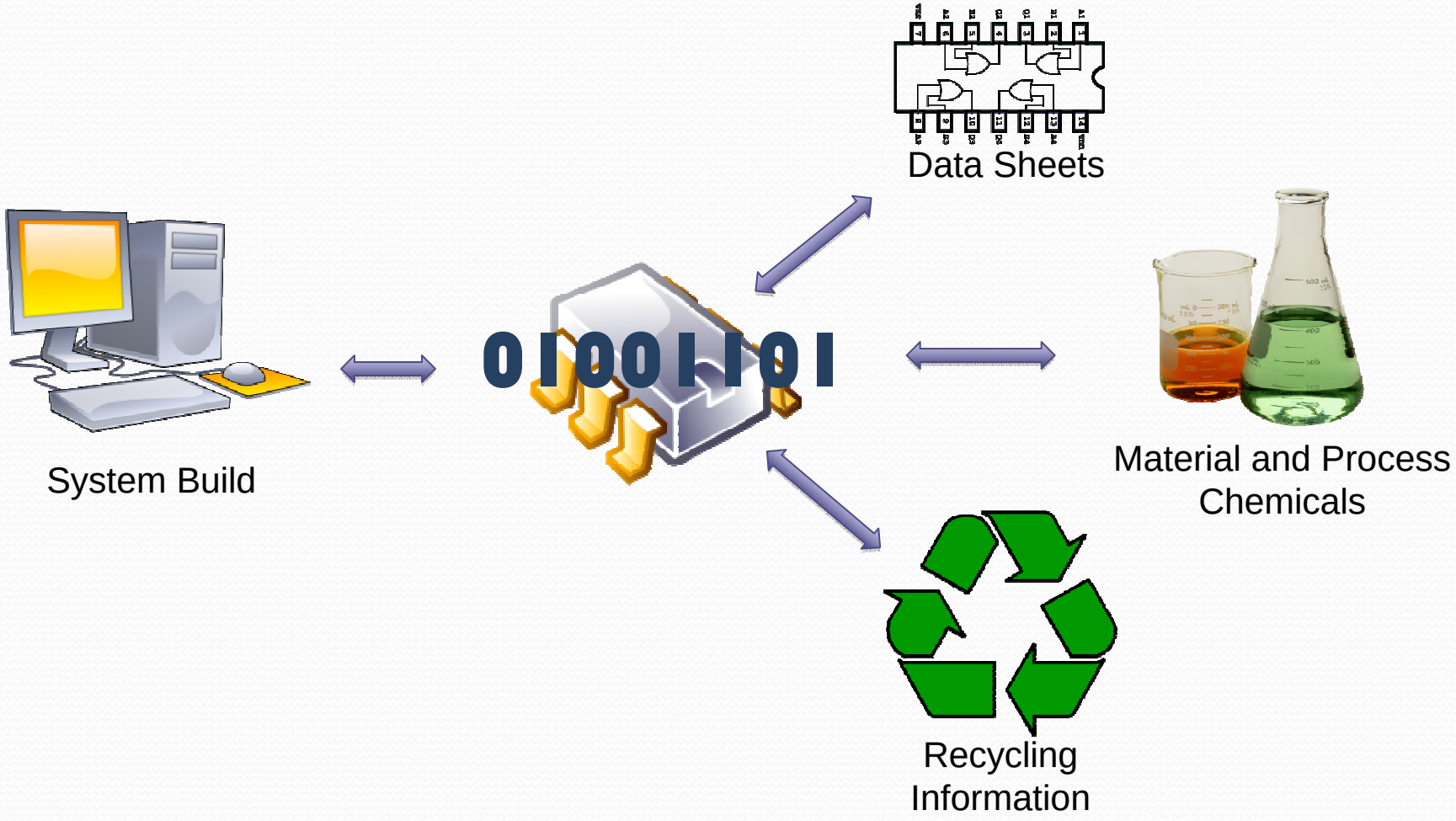
Authentication Architecture

- Centralized
- Federated

Identity Life Cycle



Identity and Uses



Identity Management System

- Identity Provisioning
- Identity Synchronization
- Access Management
- Federated Services
- Directory Services
- Auditing and Reporting

Federated IMS

Heterogeneous authentication network

- Best-of-breed
- Cost-effective for application

Flexibility

- Use of best available security technologies

Accessibility

- Communication interfaces among disparate security domains

Existing Standards

- Leverage current efforts

Standards

How can standards help?

Standard Advantage

Interoperability

- Rapid data access
- Ease communication
- Focus solutions on security

Data integrity

- Eliminates translation errors

Security

- Robustness

Customer Protection

- Confidence in anti-counterfeiting solution

Other Industries

And what we can learn

E-Authentication Guideline

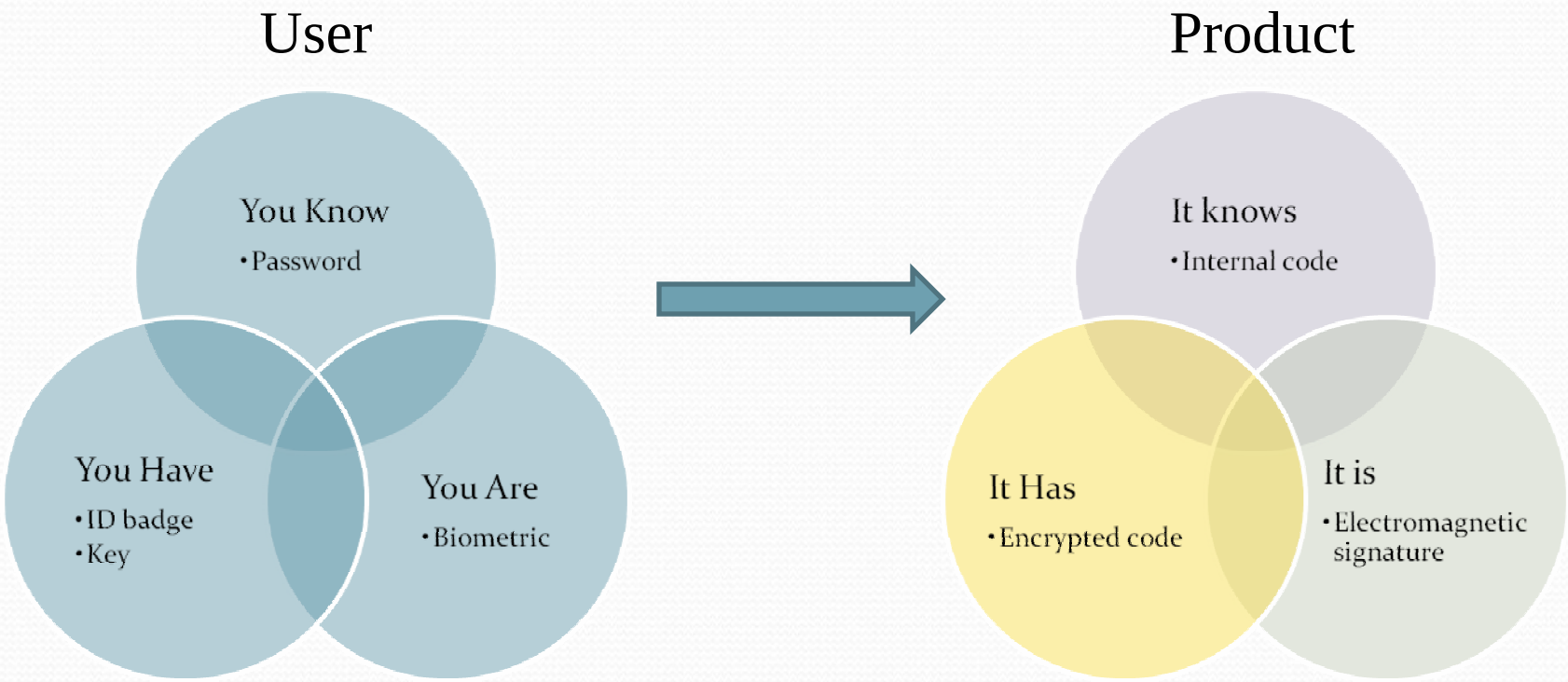
NIST 800-63 specifies Authentication Levels

Assurance Criteria:

- Tokens
- Identity proofing
- Remote authentication mechanisms
- Assertion mechanisms

Level	Assurance	Confidence
1	Tokens without identity proofing	None to little
2	Identity proofing with single-factor authentication	Some
3	Multi-factor authentication	High
4	Hard cryptographic tokens (FIPS 140-2)	Very high

Multi-Factor Authentication



Liberty Alliance

The Project:

- Global body to establish business, policy and technical standards for digital identity management
- Expert and public special interest groups, industry, government
  - Identity Assurance, Public Policy, Technology EGs
  - eGovernment, Strong Authentication, Web Services Harmonization SIGs
- Formed in 2001, by 30 organizations
- Today, it is comprised of more than 150 organizations

Specifies:

- Assurance Levels (NIST800-63)
- Criteria for meeting assurance levels
- Liability
- Governance
- Communication

Liberty Alliance

Objectives:

- Open standard-based specification for federated identity
- Interoperability testing
- Certification
- Establish best practices, rules
- Collaborate with other standards bodies, government policies
- Privacy and confidentiality

Vertical and horizontal issues:

- Networked healthcare privacy
- E-Government
- Identity theft

SAML

Security Assertion Markup Language

- For managing single sign-on (SSO) problem
- XML-based solution for web services
- SAML2

Communication among disparate security domains

- Authentication
- Attribute
- Authorization

Common Criteria

Assessment of security solutions

- Latest update CC version 3.1 in September 2007
- ISO 18045
- Comprised of:
  - Part 1: Introduction and general model
  - Part 2: Security functional requirements
  - Part 3: Security assurance requirements

Pharmaceutical

Standards

- Unique identifying code
  - 2D Matrix labels
  - Each medicine pack distributed
- Avoid issues of localized encoding approaches
- Supply chain elements
  - Wholesalers, distributors, pharmacies for traceability

Legislation (Europe)

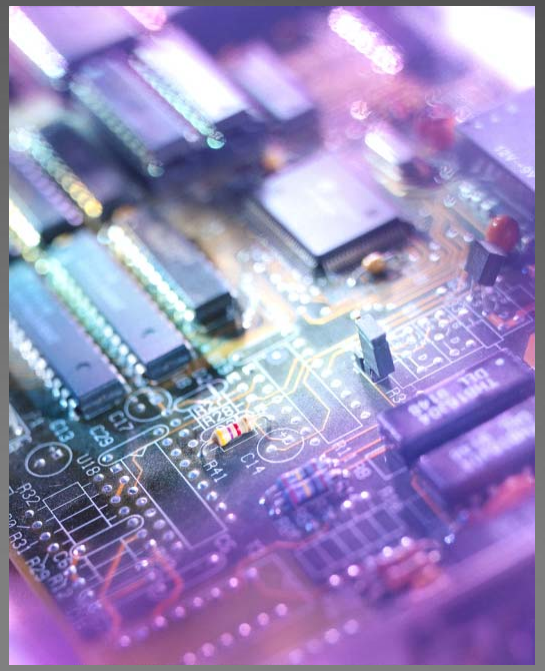
- Possible ban of re-packaging to ensure labels are not destroyed until end use

Challenges:

- Management and ownership of serialized codes
- Global parallel efforts (US, Europe, Asia)
- Cost of implementation

Electronics Industry

Current Landscape



Product Identification Efforts

Unique Identification

- SEMI Anti-Counterfeiting TF
- Product Message + ASP URL

Tracking and Traceability

- Bill of Materials (IPC 175x)
- Product life cycle information management (iNEMI – Information Management Systems TWG)

Security

- Robustness
- Compliance and certification levels

Customer Protection

- Common Criteria (ISO 18405)
- Confidence in product authentication security

SEMI Anti-Counterfeiting

Anti-Counterfeiting Task Force (ACTF)

- Enable infrastructure for encrypted codes
- Online product authentication

Standards and Efforts

- System architecture – SEMI T20-1108
- Object labeling
- ASP communication
- ASP qualifications

IPC 175x Supplier Declaration Standard

Supply chain data exchange

- 1751 is the generic declaration information
  - Business, contact, product
  - Version 2.0 draft under committee review

Supply chain communication of unique ID

- “Unique ID” element for product identifier
- Can be used to support SEMI encrypted codes

Pitfalls and Lessons Learned

Too many standards!

- Supply chain integration issues
- Interoperability
- Awareness and understanding

Slow to evolve

- Cumbersome standardization process
- Room for growth and flexibility

Security

- Security in obscurity
- Security in diversity
- Open prototyping and testing

Opportunities

Understand Market Needs

- Develop a vision for electronic product identity management
- Develop use cases for product authentication

Develop Specifications

- Develop unique IDs
- Incorporate unique IDs into current BoMs
- Leverage user authentication schemes for product authentication
- Leverage security assessment criteria for product authentication solutions

Drive Convergence

- Manage product life cycle identity information
- Standards interoperability

Innovate!