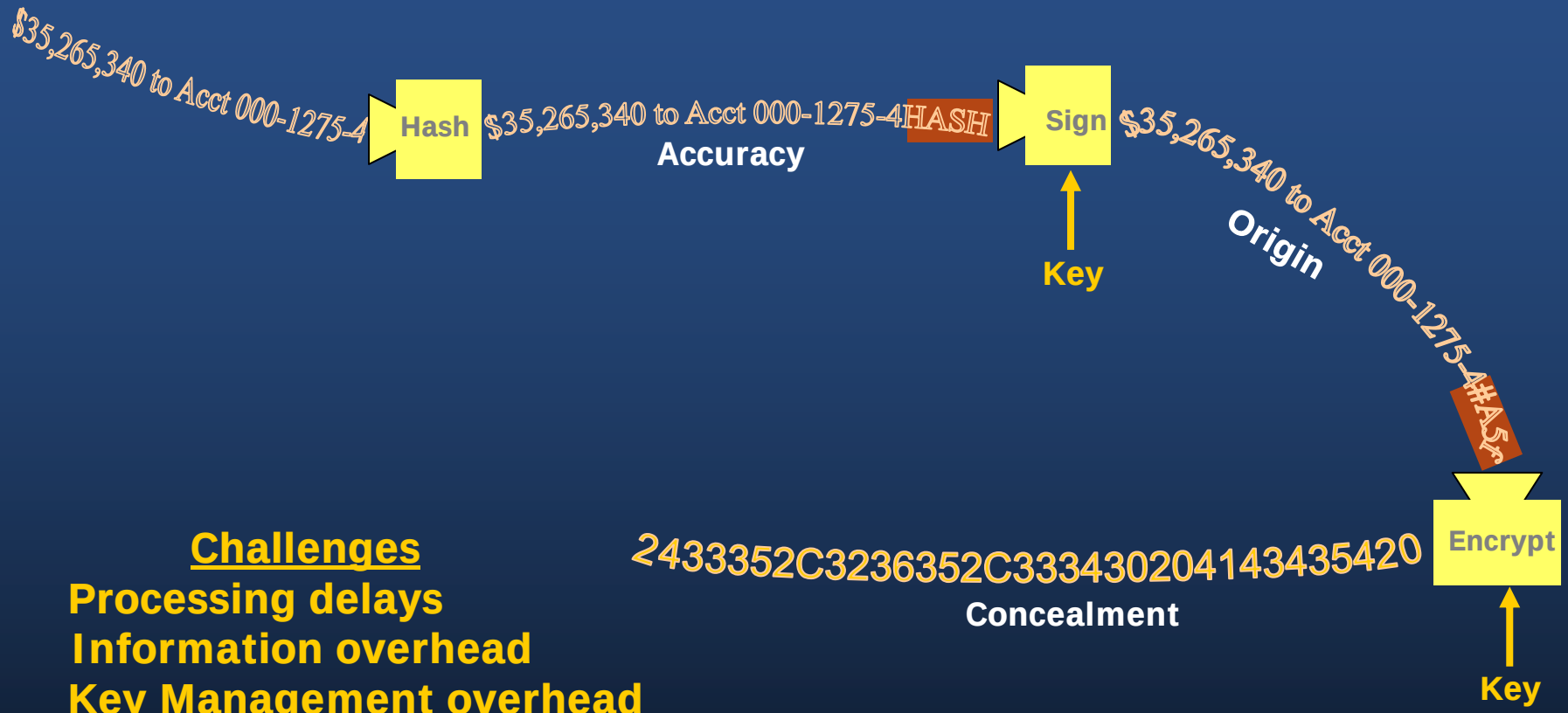
NIST
Information Technology Laboratory
(ITL)
The Cyber Maryland Showcase

NIST
National Institute of Standards and Technology

Cryptography



Challenges

- Processing delays
- Information overhead
- Key Management overhead
- Compatibility
- Erosion of security
  - Moore's Law
  - Processing efficiency (Quantum)
  - Cryptanalysis

Standards Process

- Process for standards similar to rule making process followed by regulatory agencies.
- Information gathering includes prior art, workshop results, and conducting competitions.
- Conformant to Federal policies.
- Technical input from other state and local governments, Federal agencies (e.g., NSA), domestic and foreign industry, and academia.

Process Steps

Information Gathering
Drafting
NIST Legal Review
OMB Review
Federal Register Notice
Public Review
Adjudication / Incorporation of Public Comments
Documentation of Public Comments
NIST Legal Review
Publication Decision
OMB Review
DOC Legal and Policy Reviews
OMB Review
Signature by Secretary of Commerce
Federal Register Notice
Publication by NIST

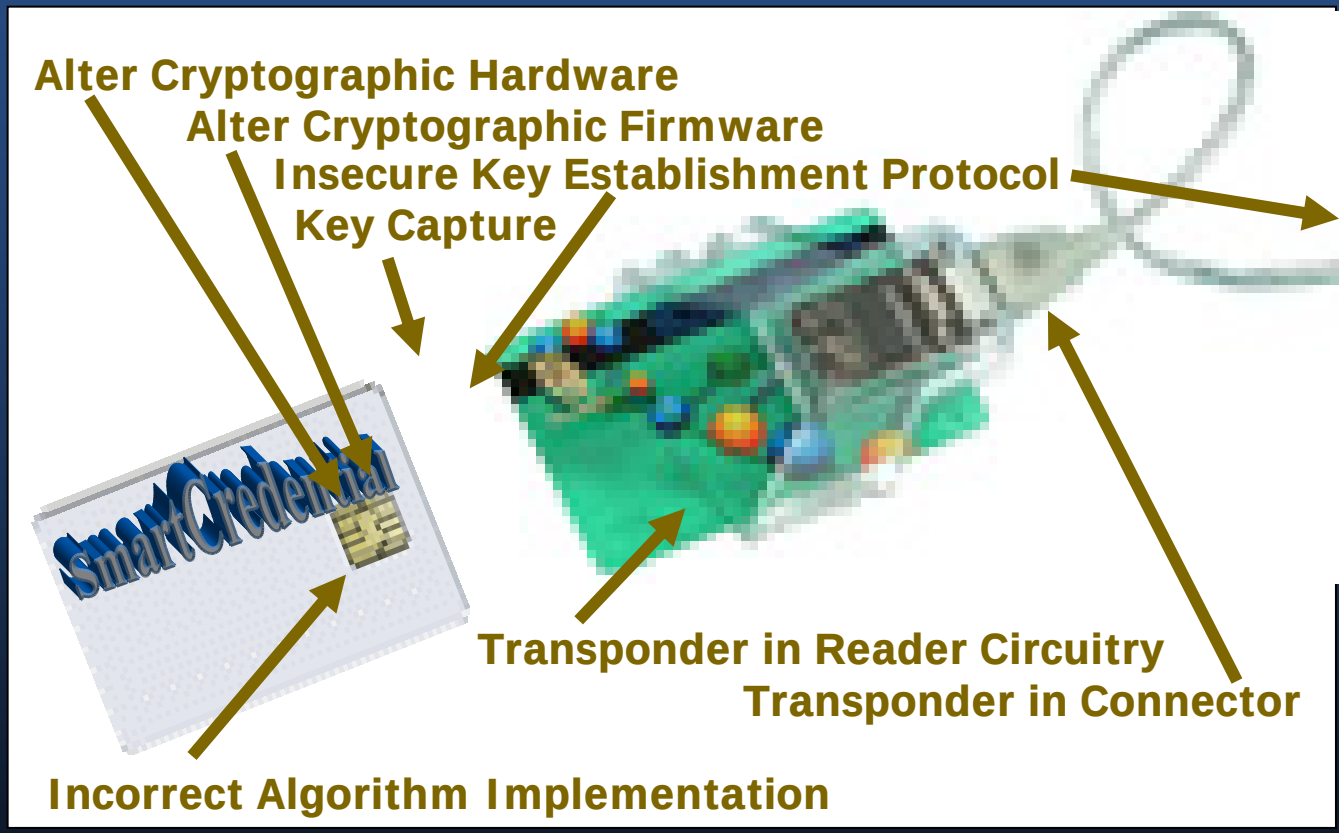
Steps in Gold Print for All Publications
Federal Information Processing Standards Only
Note: Steps can be recursive.

Implementation Concerns

Many ways to implement sound cryptographic algorithms incorrectly or in an insecure manner.

Many cases of insecure implementations.

Test and validation programs are needed to establish and maintain product assurance.



Product Validation Programs

Standards-based test and evaluation by private sector (FIPS, ISO, etc.)

Automated test tools

National Voluntary Laboratory Accreditation Program (NVLAP)

International Laboratory Accreditation Cooperation (ILAC) - Reciprocity

Government validation of laboratory reports (high-impact applications)

- **> Cryptographic Algorithm Validation Program**
- **> NIST Personal Identity Verification Validation**
- **> Cryptographic Module Validation Program**

  - **- Managed by U.S. (NIST) and Canada (CSE)**
  - **- U.S. and foreign laboratories accredited**
    - **U.S.**
    - **U.K.**
    - **Canada**
    - **Japan**
    - **Germany**
    - **Taiwan**
  - **- World-wide vendor set**

Government requirements for validated products (e.g., U.S., Japan)

NIST Partnerships

White House
- Policy
- Priorities
- Standards Coordination

Legislative Branch
- Laws and Policy
- Priorities
- Funding

State & Local Governments
- Operational Requirements
- Operational Constraints
- Technical Interchange

Federal Departments
- Standards Coordination
- Operational requirements
- Operational constraints
- Technical interchange

Foreign Organizations
- International Standards
- Product Assurance
- Technical Interchange

National Security Organizations
- Standards Coordination
- Technical Interchange/Expertise
- Threat/Vulnerability Information
- Research and Development

Academia
- Research
- Technical Interchange
- Technical Expertise

Industry
- Standards Coordination
- Technical Interchange
- Implementation Opportunities
- Implementation Constraints
- Operational Considerations
- Research and Development

Wm Curt Barker
Computer Security Division
Information Technology Laboratory
wbarker@nist.gov
301-975-8443

National Institute of Standards and Technology