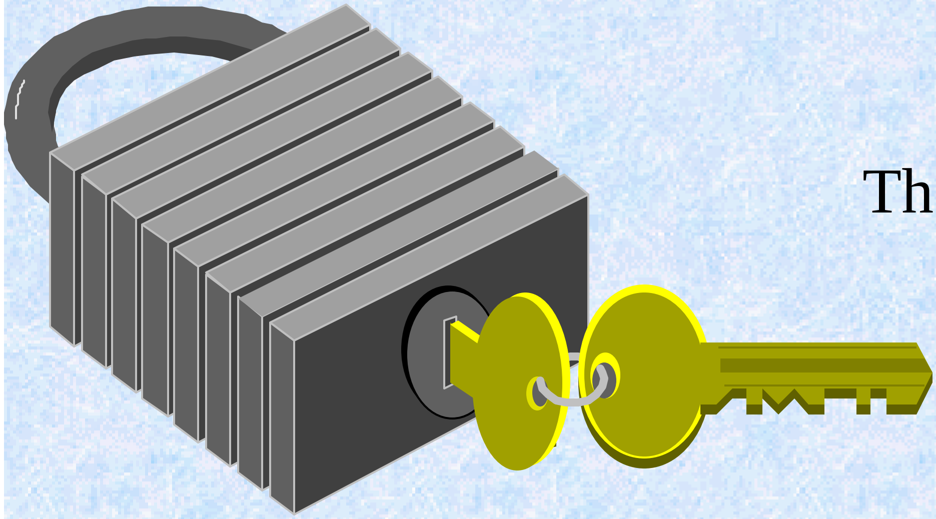
Healthcare Security: Assessing Product Compliance to Requirements

L. Arnold Johnson
National Information Assurance Partnership
National Institute of Standards and Technology

The Third National HIPAA Summit
October 25, 2001



Agenda

- Healthcare Security Dilemma
- Common Criteria Security Standard
- Defining Security Requirements
- Scheme for Validating Compliance
- Healthcare Security Examples
- Summary

The Healthcare Security Dilemma

How can the healthcare community satisfactorily demonstrate that its information technology products and systems are in compliance with policy (HIPAA, HCFA, etc.)?

The Dilemma is multifaceted

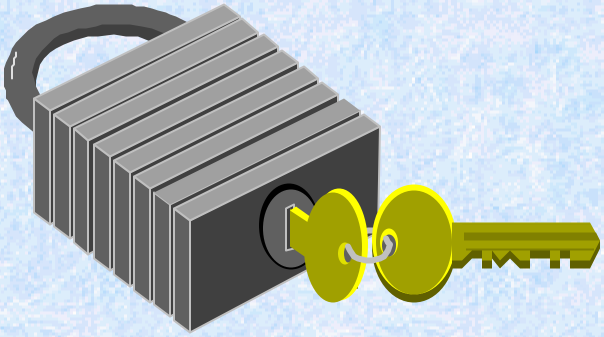
How do we:

- capture needs and concerns in implementable policy?
- translate policy into technology?
- confirm technology complies with policy ?

Security Requirements

Compliance with what???

- Healthcare IT security architecture(s)
  - operational environment
  - functional needs
  - security objectives



- Policy
  - public law
  - federal, state, local, organizational policy
  - standards
  - regulations
  - *et al*

Basic Healthcare IT Security Problem

- Lack of a common language to bridge the communication gap among HC security policy makers, standards organizations, consumers and developers
- Lack of a common structure for expressing HC security requirements and assurance
- Lack of accredited labs & recognized sources for
  - evaluating the security properties of HC products
  - validating product & system compliance

N I A P

Is there an industry-recognized methodology or mechanism to bring some coherence to this problem

?

The ***Common Criteria***

a promising, and accepted, solution

- International Standard (**ISO/IEC 15408**), *Common Criteria for Information Technology Evaluation* (CC)
- Practical way to specify and measure IT security
  - capture users’ functional and assurance requirements
  - translate policy into product/system specifications
  - guide product/system development
  - evaluate products/systems
- Flexible and adaptable to healthcare needs

The International Standard

ISO/IEC 15408

What the standard is –

- Common structure and language for expressing product/system IT security requirements (Part 1)
- Catalog of standardized IT security requirement components and packages (Parts 2 and 3)

How the standard is used –

- Develop protection profiles and security targets -- specific IT security requirements and specifications for products and systems
- Evaluate products and systems against known and understood IT security requirements

IT Security Requirements

The Common Criteria defines two types of IT security requirements--

Functional Requirements

- for defining security behavior of the IT product or system:

- **implemented requirements become security functions**

Assurance Requirements

- for establishing confidence in security functions:

- **correctness of implementation**
- **effectiveness in satisfying security objectives**

Examples:

- ***Identification & Authentication***
- ***Audit***
- ***User Data Protection***
- ***Cryptographic Support***

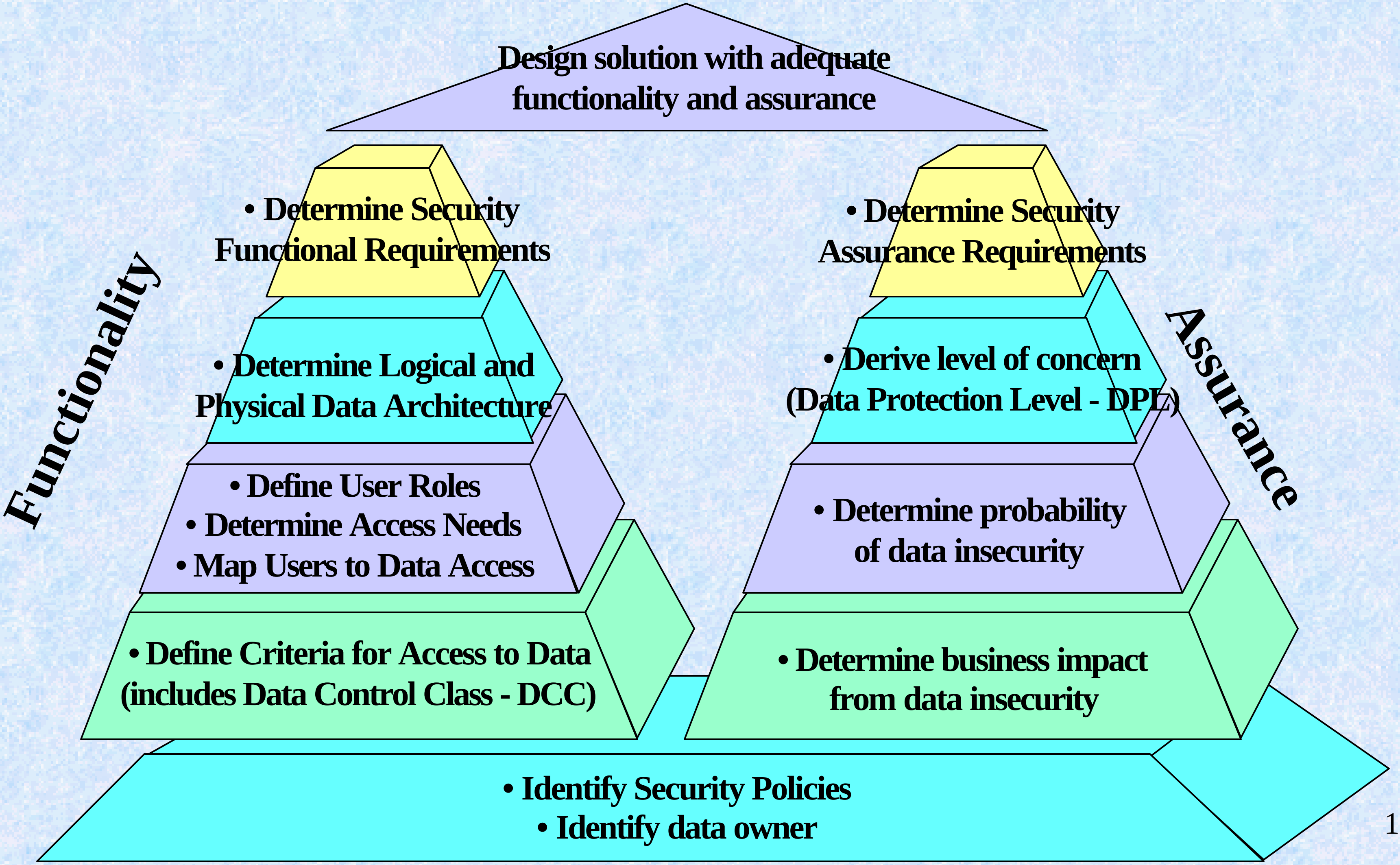
Examples:

- ***Configuration Management***
- ***Life Cycle Support***
- ***Tests***
- ***Vulnerability Assessment***

Standard for Defining Security Requirements

- ***Common Criteria*** (CC), a.k.a. ISO/IEC International Standard 15408, provides a framework for defining security requirements (both features and assurances) in IT products
- CC ***Protection Profiles*** (PP) describe generalized security requirements for a class of IT products (from consumers perspective), e.g., banking, healthcare
- CC ***Security Targets*** (ST) describe specific security claims by producers of IT products

Defining Security Requirements



Design solution with adequate functionality and assurance

Functionality

- Determine Security Functional Requirements
- Determine Logical and Physical Data Architecture
- Define User Roles
- Determine Access Needs
- Map Users to Data Access
- Define Criteria for Access to Data (includes Data Control Class - DCC)

Assurance

- Determine Security Assurance Requirements
- Derive level of concern (Data Protection Level - DPL)
- Determine probability of data insecurity
- Determine business impact from data insecurity

- Identify Security Policies
- Identify data owner

Protection Profiles (generic) & Security Targets (specific)

Consumer …..

***Protection Profile* contents**

- **Introduction**
- **TOE Description**
- **Security Environment**
  - **Assumptions**
  - **Threats**
  - **Organizational Security Policies**
- **Security Objectives**
- **Security Requirements**
  - **Functional Req’ts**
  - **Assurance Req’ts**
- **Rationale**

Developer/Vendor …..

***Security Target* contents**

- **Introduction**
- **TOE Description**
- **Security Environment**
  - **Assumptions**
  - **Threats**
  - **Organizational Security Policies**
- **Security Objectives**
- **Security Requirements**
  - **Functional Req’ts**
  - **Assurance Req’ts**
- ***TOE Summary Specification***
- ***PP Claims***
- **Rationale**

Evaluation Assurance Levels (EALs)

(Basis for Mutual Recognition)

- **Evaluation Assurance Levels & (*rough*) Backward Compatibility Comparison**

EAL	Name	*TCSEC
EAL1	Functionally Tested	
EAL2	Structurally Tested	C1
EAL3	Methodically Tested & Checked	C2
EAL4	Methodically Designed, Tested & Reviewed	B1
EAL5	Semiformally Designed & Tested	B2
EAL6	Semiformally Verified Design & Tested	B3
EAL7	Formally Verified Design & Tested	A1

***TCSEC = "Trusted Computer Security Evaluation Criteria" -- "Orange Book"**

Benefits of using the Common Criteria

- A common language for specifying security functional & assurance requirements
- A comprehensive catalogue of security requirements that
  - can be mixed/matched, extended & refined
  - can specify a product or class of products/systems

Benefits of using Protection Profiles

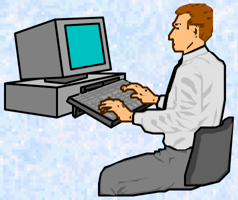
- Standard framework for capturing
  - government & social policies & regulations
  - enterprise specific policies & objectives
- Standard structure for articulating security functional & assurance requirements of solutions (products) that
  - **address specific HC security policies**
  - **meet specified HC security objectives**
  - **address specified HC risks/threats**
- Basis for verifying that products comply

Common Methodology for Evaluating IT Security Implementations

- ***Common Evaluation Methodology for Information Technology Security*** (CEM), companion document to the CC that defines a common methodology for conducting evaluations
- The CEM describes the minimum actions to be performed by an evaluator in order to conduct a CC evaluation using the criteria and evaluation evidence defined in the CC

Users of the Common Criteria

Consumers - to support the procurement of products/systems with IT security features



Product Developers and Integrators - as a basis for the development of products/systems with IT security features

Evaluators - as the basis for the evaluation of IT security products/systems

Auditors, Certifiers, Accreditors, <u>ANYONE</u> - to support specific needs for security specifications

Are there available resources to help define, assess and validate product compliance ?

Introducing NIAP

- The National Information Assurance Partnership (NIAP) is a U.S. Government initiative designed to meet the security testing, evaluation, and assessment needs of both information technology (IT) producers and consumers
- NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in fulfilling their respective responsibilities under the Computer Security Act of 1987

Program Areas

- Security Requirements Definition and Specification

  How do we tell product and systems developers what types of IT security we want?

- Product and System Security Testing, Evaluation, and Assessment

  How do we know if developers produced what we asked for?

- Information Assurance Research

  How can we improve the ways we achieve assurance in our products and systems?

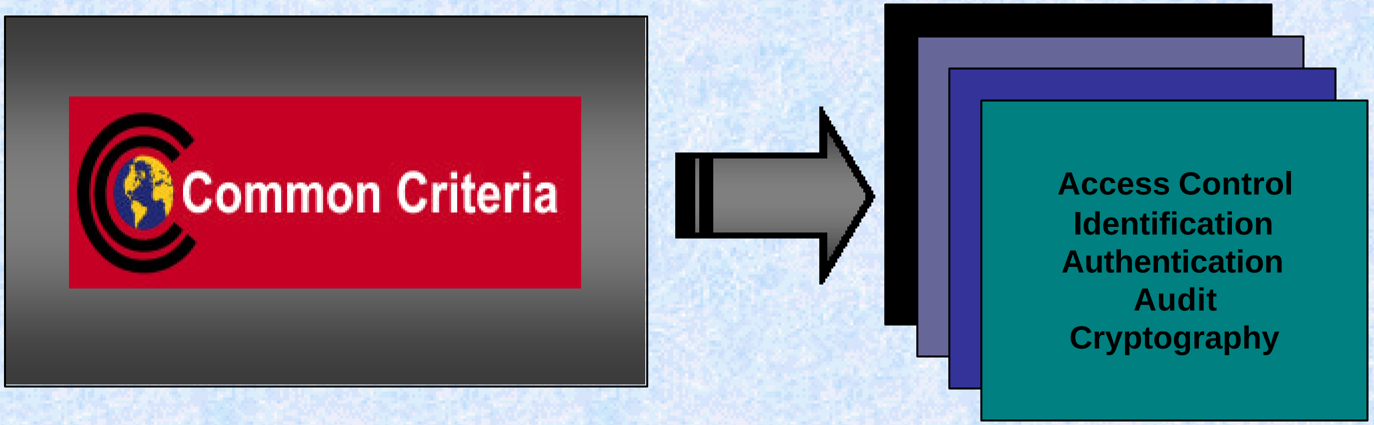
Common Criteria Evaluation/Validation Scheme (CCEVS)

- Internationally recognized program
  - that accredits commercial security evaluation labs
    - to use approved test methods e.g., CEM standard
    - to evaluate products claiming compliance to CC-based security requirements traceable to security policies
  - provides independent validation of commercial labs' evaluations
  - awards certificates to validated products

Defining Requirements

ISO/IEC Standard 15408

Protection Profiles



Access Control
Identification
Authentication
Audit
Cryptography

- ✓ Operating Systems
- ✓ Database Systems
- ✓ Firewalls
- ✓ Smart Cards
- ✓ Applications
- ✓ Biometrics
- ✓ Routers
- ✓ VPNs

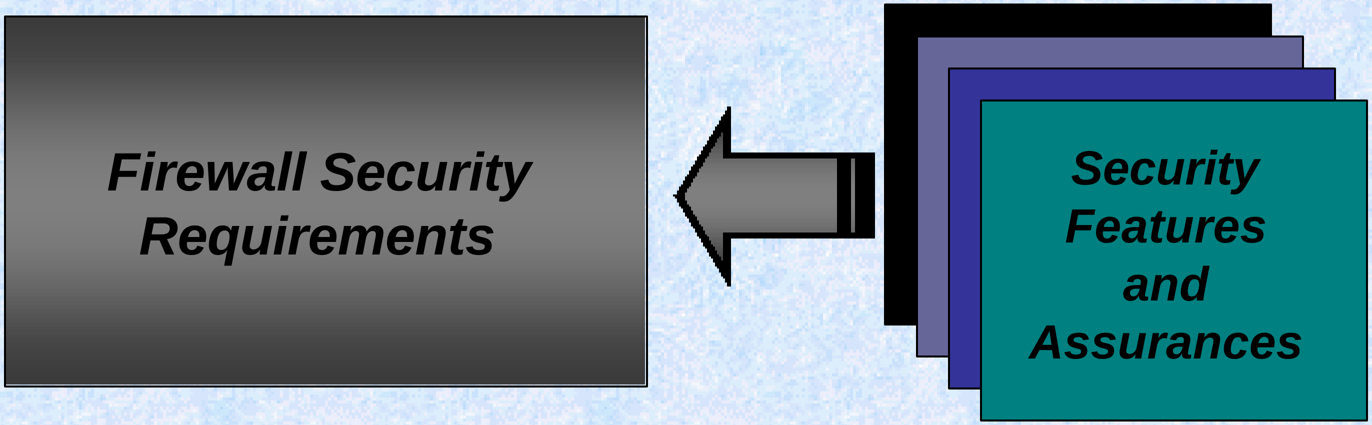
A flexible, robust catalogue of standardized IT security requirements (features and assurances)

Consumer-driven security requirements in specific information technology areas

Industry Responds

Protection Profile

Security Targets



Firewall Security Requirements

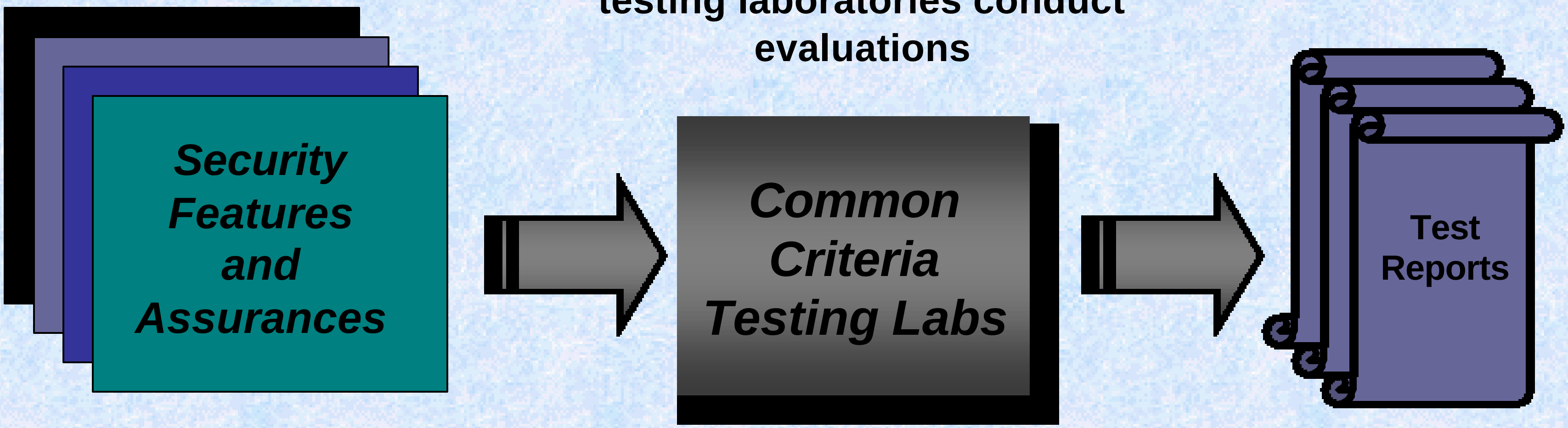
Security Features and Assurances

- ✓ CISCO Firewall
- ✓ Lucent Firewall
- ✓ Checkpoint Firewall
- ✓ Network Assoc. Firewall

Consumer statement of IT security requirements to industry in a specific information technology area

Vendor statements of security claims for their IT products

Demonstrating Conformance

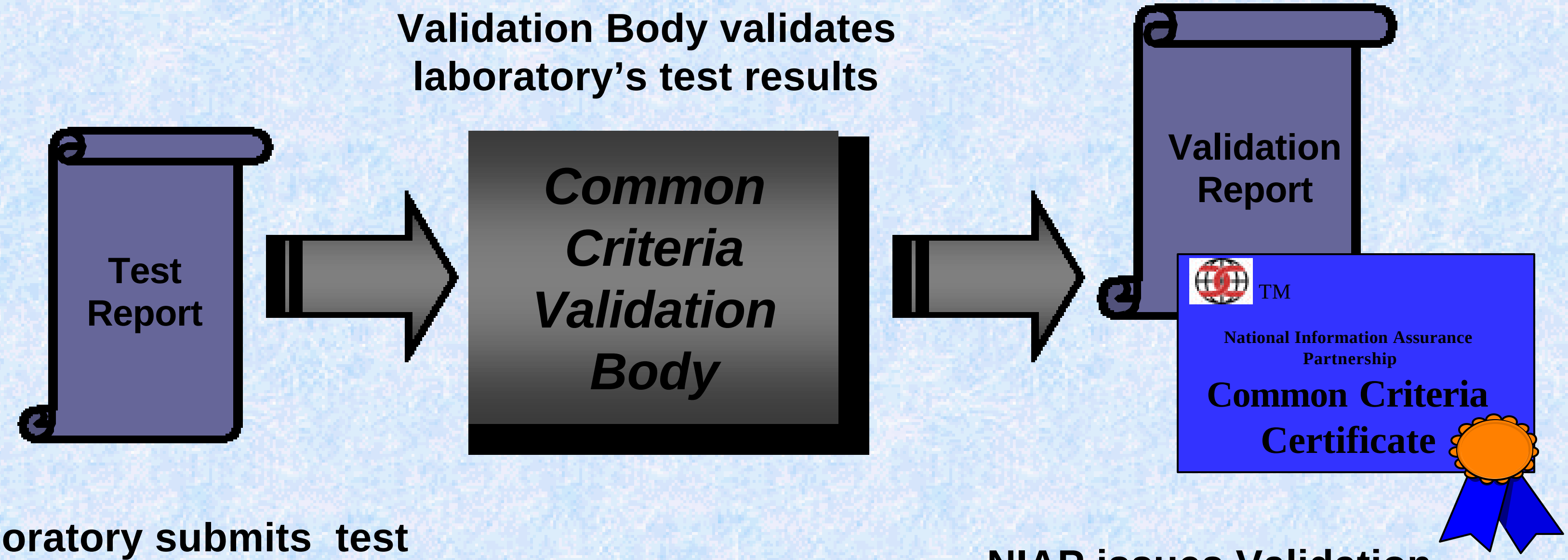

Security Features and Assurances
Common Criteria Testing Labs
Test Reports

Private sector, accredited security testing laboratories conduct evaluations

Vendors bring IT products to independent, impartial testing facilities for security evaluation

Test results submitted to NIAP for post-evaluation validation

Validating Test Results



Validation Body validates laboratory's test results

Test Report

Common Criteria Validation Body

Validation Report

TM

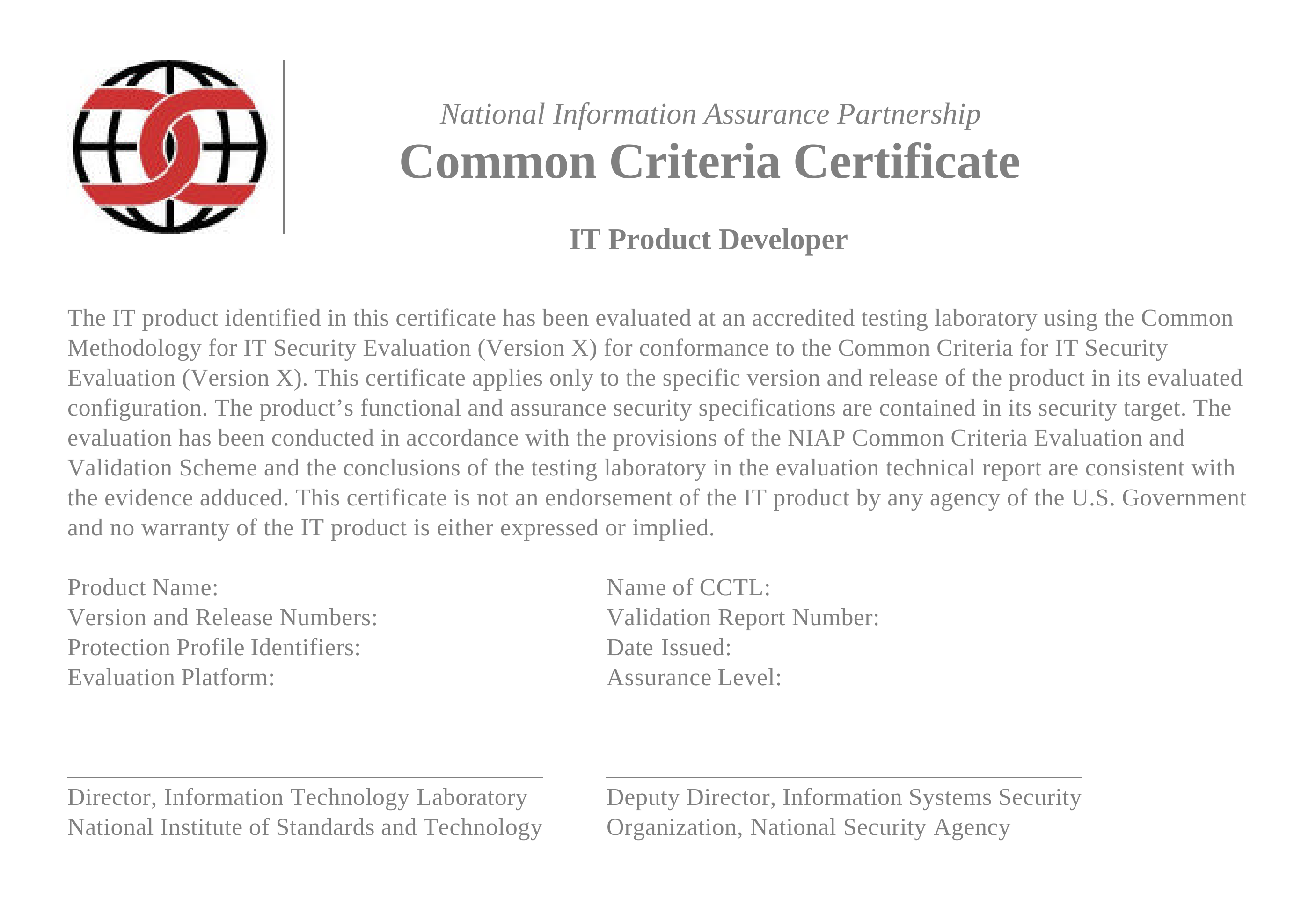
National Information Assurance Partnership

Common Criteria Certificate

Laboratory submits test report to Validation Body

NIAP issues Validation Report and Common Criteria Certificate

Common Criteria Certificate



National Information Assurance Partnership

Common Criteria Certificate

IT Product Developer

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version X) for conformance to the Common Criteria for IT Security Evaluation (Version X). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product’s functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name:
Version and Release Numbers:
Protection Profile Identifiers:
Evaluation Platform:

Name of CCTL:
Validation Report Number:
Date Issued:
Assurance Level:

Director, Information Technology Laboratory
National Institute of Standards and Technology

Deputy Director, Information Systems Security
Organization, National Security Agency

Sample NIAP Validated Product List and International MRA Seal

- Some Security Products:
  - Cisco PIX Firewall 520 (★PP Compliant) 🇺🇸
  - Lucent Managed Firewall V4.0 🇺🇸
  - ITT Dragonfly Guard G1.2 🇺🇸
  - Voltaire 2in 1 PC(TM) 🇺🇸
  - Milkyway Black Hole V3.01 E2 Firewall 🇨🇦
  - Oracle Version 7.2 on NT 3.5.1 🇬🇧
- Some Protection Profiles:
  - Controlled Access (V1.d) 🇬🇧
  - Traffic Filter Firewall for Low Risk Env. (V1.1) 🇺🇸
- Full List of Validated Products & PPs
  - http://niap.nist.gov/cc-scheme

Mutual Recognition Arrangement Seal

Mutual Recognition Arrangement

NIAP, in conjunction with the U.S. State Department, negotiated a Common Criteria Recognition Arrangement that:

- Provides recognition of U.S. issued Common Criteria certificates by 13 nations:

  Australia, Canada, Finland, France, Germany, Greece, Israel, Italy, New Zealand, Norway, Spain, The Netherlands, United Kingdom
- Minimizes need for costly security evaluations in more than one country
- Offers excellent global market opportunities for U.S. IT industry

Benefits of using CCEVS

- Increases consumer confidence about purchased products
  - **verifies products built right, do what's expected, comply with policies**
- Lowers user expenses
  - shortens acquisition cycles
    - **outsourced security testing minimizes acceptance testing**
    - **fosters "build/buy/use anywhere" strategy**
  - decrease liability costs
    - **legal: can provide "due diligence" & "best practices" evidence**
    - **insurance: potential to lower premiums**

Common Criteria Information

For more introductory info about the CC:

NIST-ITL Bulletin (11/98) , get it at:
http://csrc.nist.gov/cc/info/cc_bulletin.htm

To obtain a copy of the *CC: An Introduction* and *CC User Guide* brochures

http://csrc.nist.gov/cc/info/infolist.htm

To get sample Protection Profiles:

http://csrc.nist.gov/cc/pp/pplist.htm

http://www.iatf.net

http://niap.nist.gov/cc-scheme/PPRegistry.html

For further information on the CCEVS and Validated Products

http://niap.nist.gov/cc-scheme

http://niap.nist.gov/cc-scheme/ValidatedProducts.html

Have these concepts actually been used in healthcare ?

NIAP Healthcare Initiative

- Establish Industry Lead Forum on Privacy & Security in Healthcare (FPSH) for defining CC-based requirements (http://healthcaresecurity.org)
- Demonstrate technical value of using CC/PP paradigm as a common/internationally understood structure for specifying security requirements for HC IT systems
- Demonstrate feasibility of using CC/PP for providing traceable and documented evidence of implementation compliance to healthcare policy
- Provide healthcare community with a framework for defining & guiding construction of a family of PP's

The Forum on Privacy and Security in Healthcare (FPSH)

- Sponsored by industry and the National Information Assurance Partnership (NIAP)
- Incorporated as non-profit charitable organization
- FPSH website

(http://healthcaresecurity.org)

General Focus of the Forum

Educating healthcare industry on Common Criteria and provide a venue for defining common sets of IT security requirements and evaluation methods for assessing compliance with applicable healthcare security-related standard/laws/policies.

Strawman target for Demonstration

Construct CC PP(s) that will articulate system requirements to capture HIPAA regulatory requirements

Demonstrate how PPs and the supporting NIAP testing infrastructure can provide traceable Healthcare Security Information Systems requirements from policies through to product/system compliance

HIPAA Security Requirement Areas Where CC Primarily Applicable (*)

- Administrative Procedures
- Physical Safeguards
- Technical Security Services (*)
- Technical Security Mechanisms (*)

Status of Common Criteria Healthcare Examples

- **HC Methodology** *“Draft Development of a Methodology & Reference Architecture for Construction of Security Protection Profiles for Healthcare Information Systems”* [Scheduled Revision 03/02]
- **HCFA based** *“Draft Security Functional Package for Systems Transmitting Sensitive HCFA Data (STS-HCFA)”* [Scheduled Revision 12/01]
- **HIPAA based** *“Functional Profile for Healthcare Provider Intranet with Limited Internet Exposure”* [Scheduled Revision 01/02]
- **HC Application Protection Profile - HIPAA based**

  “Patient Point-of-Care Admission, Discharge & Transfer” [Scheduled Revision 01/02]

How can the industry [healthcare org, vendors/developers and certifying organizations] take part in developing a set of solutions?

Send contact info and queries to:

info@healthcaresecurity.org

For More Information

- Forum on Privacy and Security in Healthcare - http://www.healthcaresecurity.org
- NIAP Website http://niap.nist.gov
- NIAP interim Protection Profile Registry http://csrc.nist.gov/cc/pp/pplist.htm
- Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, NIST Special Pub 800-23, August 2000

  http://csrc.nist.gov/publications/nistpubs

Summary

- ISO/IEC 15408 *Common Criteria for IT Security Evaluation* and NIAP IT product/system evaluation and validation infrastructure an approach for “due diligence” in HC IT security
- NIAP providing sample protection profiles for selected HC environments as proof of concept for healthcare
- Demonstrating CC/PP paradigm tool for providing traceable and documented evidence of implementation of high level healthcare policy (i.e., HIPAA & HCFA) to product compliance

Contact Information

For further information contact:

L. Arnold Johnson, CISSP
National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Dr. Building 820 (NIST North) Stop 8930
Gaithersburg, MD 20899

email: arnold.johnson@nist.gov phone: (301) 975-3247
web: http://niap.nist.gov/cc-scheme fax: (301) 948-0275