

NVLAP Program for Cryptographic Module Testing

September 2004



National Voluntary Laboratory Accreditation Program



Jeffrey Horlick

**National Institute of Standards and Technology
National Voluntary Laboratory Accreditation Program
(NIST / NVLAP)**

**Building 820 Room 287
100 Bureau Drive Stop 2140
Gaithersburg, MD 20899-2140**

Phone: 301.975.4020

Fax: 301.926.2884

E-mail: jeffrey.horlick@nist.gov

URL: <http://www.nist.gov/nvlap>

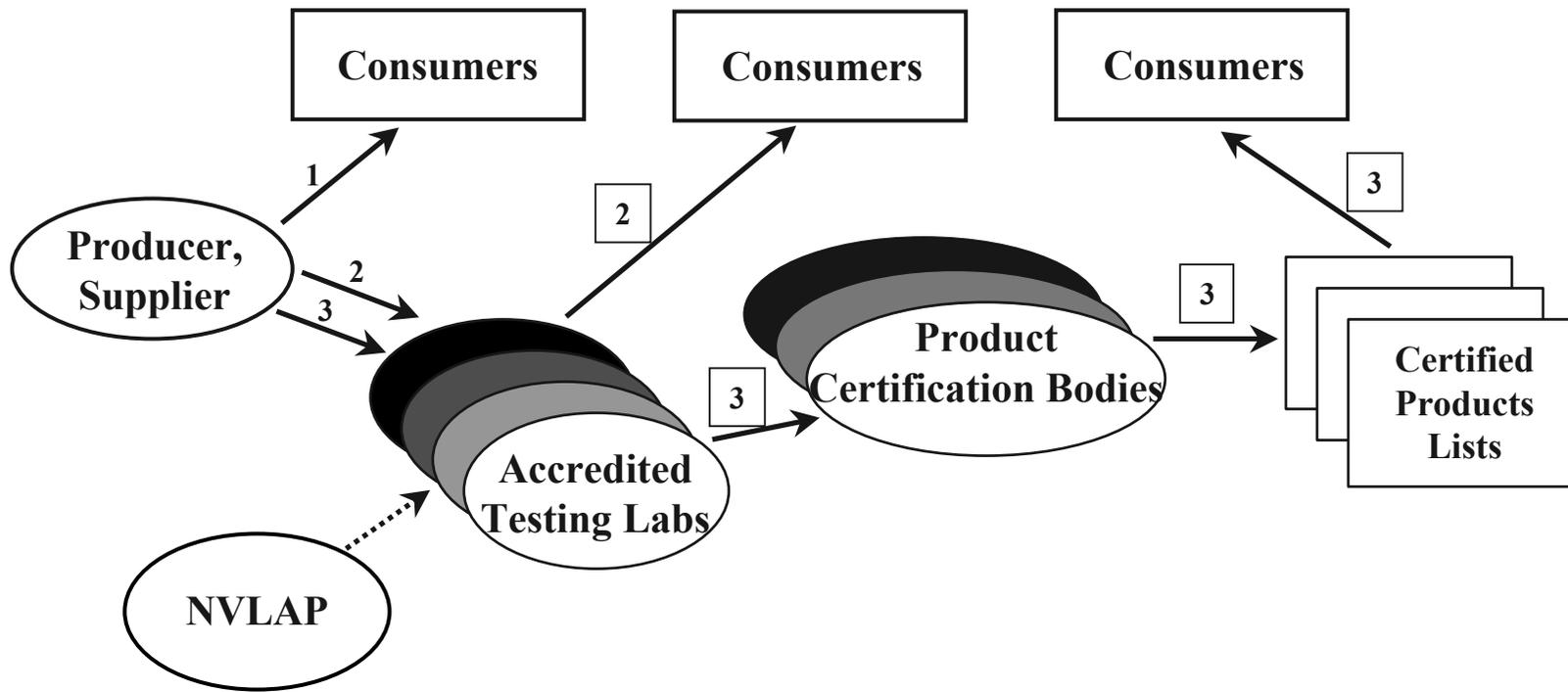
Why Laboratory Accreditation?

- So you don't have to worry.
 - Confidence - it has been done right
 - Competence - get the right answer
 - Equivalence - get the same answer
 - Independence - nothing else is going on
 - Appropriateness - fit for purpose
 - Repeatability - get the same answer twice
 - Reproducibility - others get same answer

Why Harmonized Standards?

- So you can talk to each other
- So you can do business with each other

Paths to Consumer

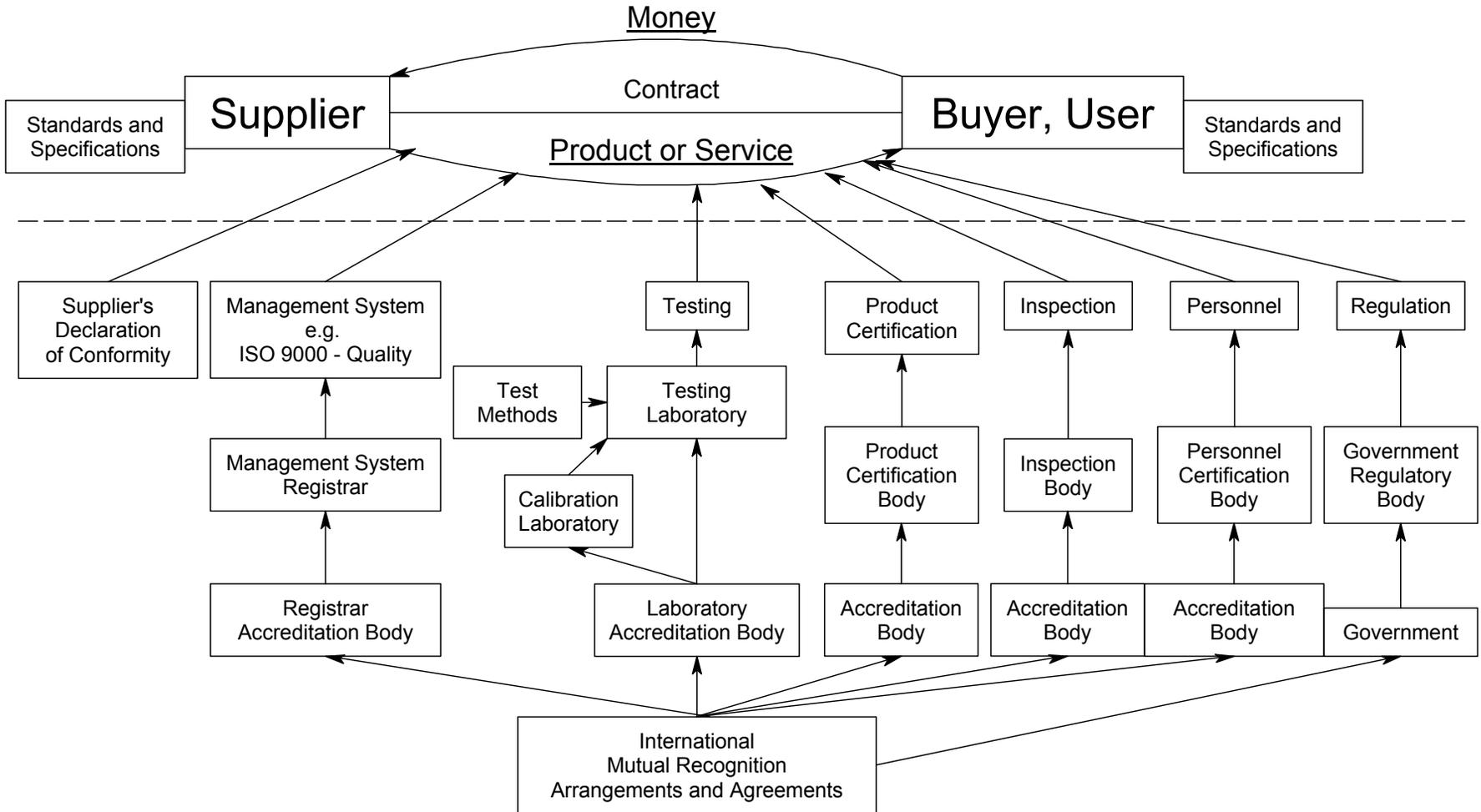


Path 1: Declaration of Conformity

Path 2: Conformance demonstrated by testing in accredited laboratory

Path 3: Conformance demonstrated by testing and product certification

DOMESTIC AND INTERNATIONAL TRADE



CONFORMITY ASSESSMENT

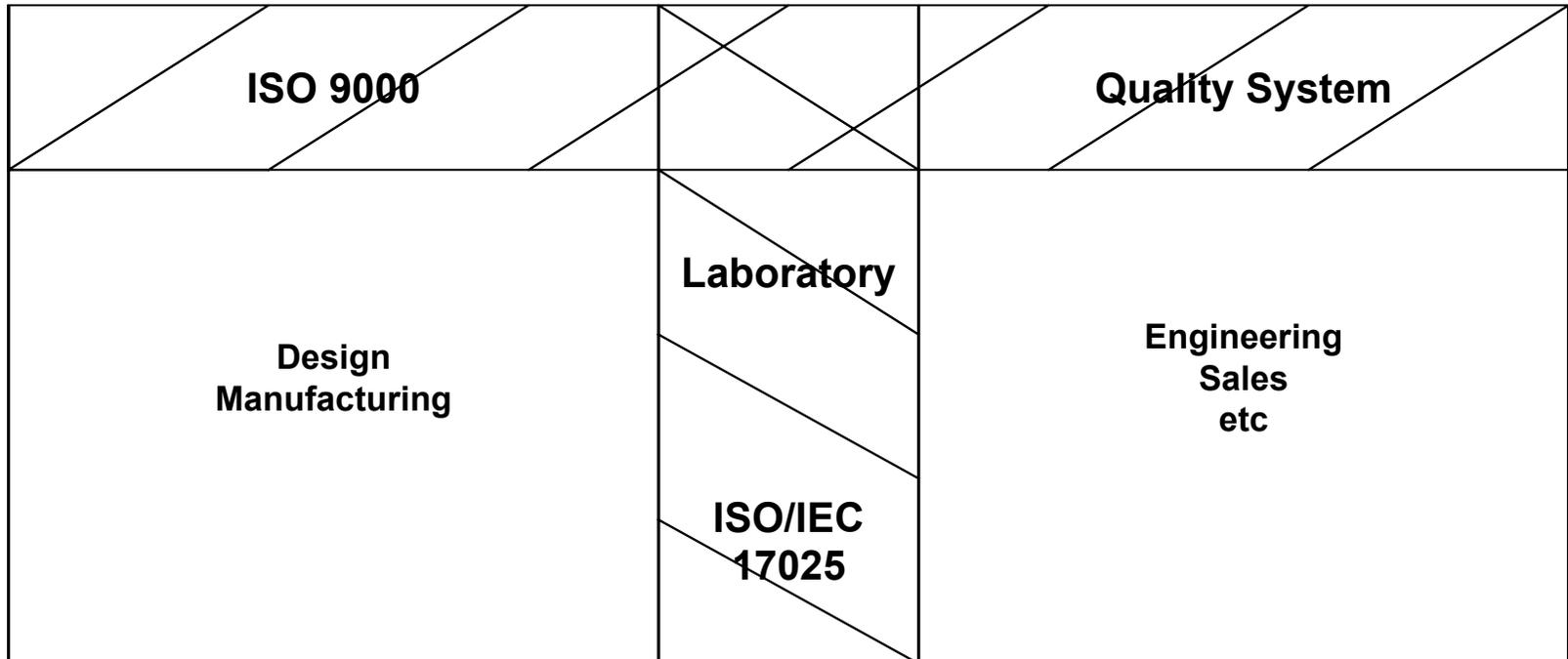
jh-20031218

Conformity Assessment - ISO Guides and Standards

Testing and Calibration Laboratories 1	Product Certification Bodies 2	Management Systems Registrars - Quality and Environment 3	Inspection Bodies 4	
Recognition Body (ILAC P1, APLAC MR001, EA-2/02)	Recognition Body (No ISO Guides or Standards)	Recognition Body (No ISO Guides or Standards)	Recognition Body (No ISO Guides or Standards)	A
Accreditation Bodies (ISO/IEC Guide 58:1993)	Accreditation Bodies (ISO/IEC Guide 61:1996)	Accreditation Bodies (ISO/IEC Guide 61:1996)	Accreditation Bodies (ISO/IEC TR 17010:1998)	B
Accredited testing and calibration laboratories (ISO 17025:1999 previously ISO/IEC Guide 25)	Product certification Bodies (ISO/IEC Guide 65:1996)	Registrars (ISO/IEC Guide 62:1996, ISO/IEC Guide 66:1999)	Inspection Bodies (ISO 17020:1998)	C
Samples (Test methods and sampling methods)	Products and services (Appropriate product or service standards)	Companies or organizations (ISO 9000, ISO 14000, or equivalent)	Products (Appropriate product standards)	D

ISO 9000 and ISO/IEC 17025

ISO 9000 is a stripe across the top of an organization



ISO/IEC 17025 is a stripe from top to bottom
covering the entire laboratory

International Mutual Recognition Arrangements (MRA)

World MRAs:

- International Laboratory Accreditation Cooperation (ILAC)
for testing and calibration laboratories
<<http://www.ilac.org/>>
- International Accreditation Forum (IAF)
for QMS, EMS, and product certification
<<http://www.iafinc.org>>

(Quality Management System, Environmental Management System)

NVLAP Programs (LAPS) for Information Technology Security Testing

- NVLAP accredits laboratories for testing to:
 - Federal Information Processing Standard (FIPS) 140-1 and 140-2 for cryptographic modules
details: <http://www.nist.gov/cmvp>
 - ISO/IEC 15408 Common Criteria
details: <http://niap.nist.gov/cc-scheme/> and <http://niap.nist.gov/index.html>

Program Specific Requirements for Cryptographic Module Testing LAP

- NIST Handbook 150 *NVLAP Procedures and General Requirements* (contains ISO/IEC 17025)
- All requirements of the CMVP
- NIST Handbook 150-17 *Cryptographic Module Testing* extends and defines Handbook 150 specifically for this program
- Proficiency Testing is designed specifically for this program
- Technical experts are trained in the NVLAP methodology and to assess to ISO/IEC 17025

Accreditation to ISO/IEC 17025:1999

- Review of quality system: Quality Manual, Procedures, Instructions, Records
- On-site assessment by a team of peer technical experts
- Participation in proficiency testing
- Evaluation of the above by NVLAP team
- Feedback to the laboratory
- Corrective action by the laboratory

Proficiency Testing

- An integral part of the accreditation process - customized for field
- A means of periodically checking laboratory performance and ability
- Required for initial and/or continuing accreditation

ISO 17025 - Management Requirements (Section 4 of NIST Handbook 150)

- Organization
- Quality system
- Document control
- Review of requests, tenders and contracts
- Subcontracting of tests and calibrations
- Purchasing services and supplies
- Service to the client
- Complaints

ISO 17025 - Management Requirements

cont'd

- Control of nonconforming testing and/or calibration work
- Corrective action
- Preventive action
- Control of records
- Internal audits
- Management reviews

ISO/IEC 17025 -Technical Requirements (Section 5 of NIST Handbook 150)

- General - factor contributing to correctness and reliability
- Personnel
- Accommodation and environmental conditions
- Test and calibration methods and method validation
- Equipment

ISO/IEC 17025 -Technical Requirements cont'd

- Measurement traceability
- Sampling
- Handling of test and calibration items
- Assuring the quality of test and calibration results
- Reporting the results

Additional NVLAP requirements

- Referencing NVLAP accreditation (use of logo and “NVLAP”)
- Implementation of traceability policy
- Approved Signatory
- Authorized Representative(s)

New Applicants for Accreditation

- Send application to NVLAP including:
 - General Application Forms
 - Program Specific Application Form
 - Fees
 - Quality Manual
- Quality documentation review by assessors
- Written exam Proficiency Test
- On-site Assessment with Round Table Quiz
- Proficiency testing of artifact after on-site visit
- Resolution of all non-conformances
- NVLAP review and grant of accreditation

Typical On-site Visit - conducted every other year (after initial two)

- Team of two assessors for 1 1/2 days
- Entry meeting with lab management
- Review quality system documentation including, records, personnel folders, technical documentation, internal audits, management reviews
- Examine facilities, hardware, software,..
- Staff interviews on all aspects of standards and testing with appropriate demonstrations

Typical On-site Visit - conducted every other year - cont'd

- Proficiency testing
- Exit meeting
 - On-Site Assessment Report given to lab
 - Required written responses to NVLAP are discussed

Quality System documentation includes (but is not limited to)

- Quality manual
- Policies, objectives, commitments
- Procedures - management and technical
- Instructions - management and technical
- Records - management and technical
- Roles and responsibilities
- Organization charts - inside laboratory boundary and laboratory's place in larger organization
- Complaints log

Proficiency Testing

- Before the on-site visit
 - A written, essay-type examination is sent to the laboratory
 - The laboratory chooses who works on exam
 - Laboratory has approximately one week to finish
 - Results returned to NVLAP and reviewed by assessors before on-site visit
 - If the laboratory does not perform satisfactorily, the on-site visit will be delayed

Proficiency Testing

- During the on-site visit
 - Assessors hold a round-table quiz / interview with entire staff
 - An artifact is given to the laboratory for testing after the on-site visit. Instructions are discussed. One CMVP person will act as the vendor. Artifact is tested by lab while interacting with “vendor” and validation authority.
- After the on-site visit
 - The artifact test is reviewed

Granting Accreditation

- NVLAP reviews all information with input from assessor team
- All non-compliances must be resolved
- NVLAP grants accreditation for one year
- Renewal each year with on-site every-other year (after initial and first-year onsite assessments)

International Laboratory Accreditation Cooperation (ILAC) Brochures

- Why Use An Accredited Laboratory?
- Why Become An Accredited Laboratory?
- How Does Using an Accredited Laboratory Benefit Government & Regulators?
- The Advantages of Being An Accredited Laboratory

<http://www.ilac.org/> see Publications
available in English, Russian, Japanese, Spanish, Chinese

NVLAP Programs for Information Technology Security Testing

The screenshot shows a Netscape browser window displaying the NIST website for Cryptographic Standards and Validation Programs. The browser's address bar shows the URL <http://csrc.nist.gov/cryptval/>. The page features a blue sidebar with navigation links such as 'Cryptographic Module Validation Program', 'Standards and Their Related Documents', 'Validation Lists', 'Testing Laboratories', 'Announcements', 'Notices', 'FAQs', 'Helpful Documentation', 'Contacts', 'Computer Security Resource Clearinghouse', and 'NIST'. The main content area has a header with the 'Cryptographic Module Validation Program' logo and the NIST logo. A prominent red text box states: 'FIPS 140-2 is now in effect. However, Agencies may continue to purchase, retain and use FIPS 140-1 validated modules.' Below this, there is a section for the 'CMVP Symposium 2004' held from September 14-15, 2004, at the DoubleTree Hotel & Executive Meeting Center in Rockville, MD. The page also includes a paragraph about the Computer Security Division at NIST and lists 'Cryptographic Modules' and 'Cryptographic Algorithms' with links to various FIPS standards like FIPS 140-2, FIPS 140-1, FIPS 197, and FIPS 46-3.

NVLAP Programs for Information Technology Security Testing

CCEVS Website - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Netsite: http://niap.nist.gov/cc-scheme/ What's Related

THE COMMON CRITERIA EVALUATION AND VALIDATION SCHEME
NIAP Home CCEVS Home About Us Contact Us Help Site Map
SECURE SYSTEMS FOR THE NEW MILLENNIUM
Aug 27, 2004

Search NIAP CCEVS
Go

The Big CCEVS Picture
■ Defining the CCEVS
■ CCEVS Objectives
■ Eval/Validation Primer
■ CCEVS Validation Body
■ Historical Perspective
■ Guidance to Consumers
■ CC Testing Labs (CCTL)
■ Candidate CCTLs
■ CCRA & Partners
■ Acronyms & Terms
■ Upcoming Events
■ The OR/OD Process
■ What's New **UPDATED!**

CCEVS Products
■ Validated Products List
■ Validated Protection Profiles
■ Products in Evaluation
■ PPs in Development
■ Archived Validated Products

Docs & Guidance
■ FAQs
■ Scheme Policy Letters
■ Scheme Publications
■ CC/CEM Documentation
■ Forms
■ LabGrams

Other Useful Links
■ Precedent Database

VALIDATED PRODUCTS
A CALL FOR PRODUCTS
Available products to assist in making a more secure infrastructure.

- ▶ VPL (by Product Type)
- ▶ VPL (by Assurance Level)
- ▶ VPL (by Product Name)
- ▶ VPL (by Vendor)
- ▶ Archived Evaluated Products
- ▶ Products in Evaluation
- ▶ Validated Protection Profiles
- ▶ PPs in Development

VALIDATING IA AND IA-ENABLED PRODUCTS
THE PROCESS
Boosting consumer confidence through evaluation and testing of vendor products

- ▶ Getting a Product Evaluated
- ▶ Finding a CCTL
- ▶ Getting a CCTL Accredited

COMMUNITIES OF INTEREST & RELATED POLICIES
Policy that influences our adherence to the Common Criteria

- ▶ DOD Directive #8500.1
- ▶ DOD Instruction #8500.2
- ▶ NSTISSP No. 11, Revised Fact Sheet (July 2003) **NEW**
- ▶ NSTISSP No. 11 Fact Sheet (Jan 2000)
- ▶ NIST Spec Pub 800-23
- ▶ NSD 42
- ▶ NSTISSAM Compusec/1-99
- ▶ USAF CIO Memorandum
- ▶ Pres. Decision Directive 63
- ▶ For a comprehensive listing other pertinent IA-related docs, [Click Here.](#)

Document: Done
Start | Horlick, Jeffrey ... | Eudora | C:\Documents a... | Lab Accred in US... | CCEVS Website... | 5:41 PM