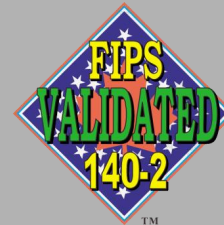# Cryptographic and Security Testing Laboratory

Deputy Laboratory Director, CST Laboratory Manager

About our Cryptographic and Security Testing Laboratory

- Bringing together a suite of conformance testing programs from agencies including NIST, CSE and the GSA. atsec offers

  – Quality

  – Expertise and experience

  – Specialist knowledge

NVLAP LAB CODE 200658-0

CST= Cryptographic and Security Testing

NVLAP= National Voluntary Laboratory Accreditation Program

CST Lab History

- **2000:** atsec information security founded
  - Started with Common Criteria
- **2005:** atsec establishes a CST Lab, accredited under NVLAP for
  - CMVP
  - CAVP
- **2008:** CST Laboratory scope expands with
  - NPIVP
  - SCAP
  - GSA FIPS 201 EP
- **2012:** CST Laboratory scope expands with
  - TWIC (Until 2015)

atsec's CST Conformance Testing Laboratories

- **NIST's Cryptographic Module Validation Program**
  - FIPS 140-2

  CMVP

- **NIST's Cryptographic Algorithm Validation Program**
  - AES, TDES, Hash, RNG, RSA etc

  CAVP

- **NIST's Personal Identity Validation Program**
  - FIPS 201, Smartcard Applet and middleware

  NPIVP

- **GSA's FIPS 201 Evaluation Program**
  - FIPS 201 related procurement (ID related products)

  GSA FIPS 201 EP

- **NIST's Security Content Automation Program**
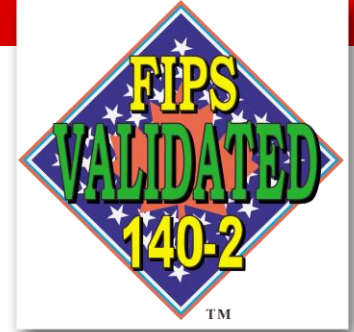 - Supporting Federal Desktop Core Configuration, Tools capabilities and components

  SCAP

Cryptographic Module Validation Program (CMVP)

- Operated in partnership by NIST's Security Management & Assurance group, and Canada's CSE

- Provides certification for conformance to the NIST standards for cryptographic modules:

  – FIPS 140-2

  – Products using cryptography and used in the U.S. Federal arena are mandated to comply.

- Used in a variety of other areas

  – U.K. And Japan Government

  – Digital Cinema specification

  – Banking and Financial

Cryptographic Algorithm Validation Program (CAVP)

- Operated by NIST's Security Management & Assurance group

- Performs validation of implementation testing of NIST Approved algorithms

  - NIST statistics have shown that close to 25% of cryptographic algorithms are implemented incorrectly.

- Algorithm Validation is performed in support of:

  - FIPS 140-2

  - PCI assessment

  - Voting systems

  - Financial Industry

  - Many other software assurance programs

FIPS Approved/NIST Recommended Cryptographic Algorithms

Symmetric key
☐ Triple DES (TDEA) (SP 800-67)
☐ AES (FIPS 197)
☐ EES - Skipjack (FIPS 185)
Asymmetric key
☐ DSA2 ☐ RSA2 ☐ ECDSA2 (FIPS 186-3)
☐ Digital Signature Standard (DSS) (FIPS 186-2)
Message Authentication
☐ CMAC (SP 800-38B)
☐ CCM (SP 800-38C)
☐ HMAC (FIPS 198)
☐ GCM and GMAC (SP 800-38D)

Hash
☐ SHA-1,224,256,384,512 (FIPS 180-3)
Random Number Generators
☐ Random Number Generation for DSA (FIPS 186-2)
☐ RNG for ECDSA (ANSI X9.62)
☐ RNG for RSA (ANSI X9.31)
☐ DRBG deterministic random bit generator (SP 800-90)
Key Management
☐ KAS FFC ☐ KAS ECC (SP 800-56A)

NIST's Personal Identity Verification Program (NPIVP)

- Operated by NIST's Systems & Emerging Technologies Security Research group

- Validate the compliance/conformance of two PIV components --PIV middleware and PIV card application with the specifications in NIST SP 800-73

- Provides assurance that the set of PIV middleware and PIV card applications that have been validated by NPIVP are interoperable
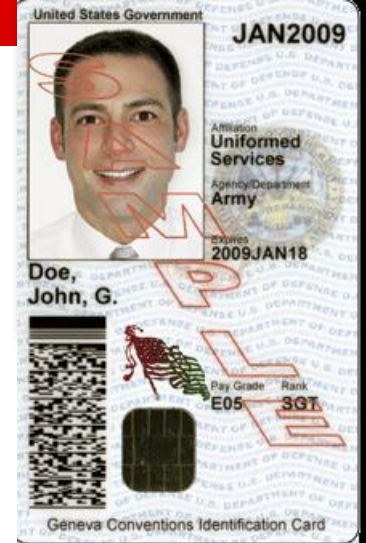
Security Content and Automation Protocol (SCAP)

- Conformance testing offered by NIST's Information Technology Laboratory

- In support of the Federal Desktop Core Configuration and vulnerability management

"Information technology providers must use SCAP validated tools, as they become available, to certify their products do not alter these configurations, and agencies must use these tools when monitoring use of these configurations." - U.S. Office of Management and Budget

GSA FIPS 201 EP

- The General Services Administration (GSA), is the executive agent for acquisition of HSPD-12 products and services

- Focuses on interoperability and performance testing

- Applies to all vendors that *submit* or *intend to submit* a proposal to sell products/services on the GSA Blanket Purchase Agreement (BPA) for FIPS 201 Approved Products/Services under Information Technology (IT) Schedule 70, Special Item Number (SIN) 132-60

atsec CST Lab Services

Training and Testing Support

Readiness Assessment

Conformance Consulting

Conformance Testing

Corporate Certification Strategy

Readiness Assessment for FIPS 140-2

- A readiness assessment helps
  - Establish a certification strategy
  - Establish boundaries of the product for optimal testing projects
  - Discover any gaps and discuss remediation
  - Introduce the developer and testing teams, establishing good rapport
  - Allow atsec to estimate costs and hence offer a fair fixed price
  - Perform basic training
- Typically 1 or 2 days duration onsite, the report follows within 2 weeks

Training for FIPS 140-2
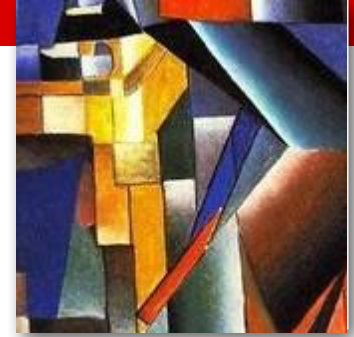
- We offer technical training for your team
  - Introductory workshop
    - suitable for business managers (2 hrs- ½ day)

  - Developer training
    - suitable for development staff involved in validation projects (1 - 5 days, Architecture, Hardware and Software)

  - Workshops on technology-specific IT security

  - Workshops on standards transitions

Conformance Testing

- Resulting in a certificate for your products

- atsec's commitment
  - On-time delivery
  - Full support for your team
  - Experts who actively follow the programs
 - Negotiation with the programs to solve technical problems

Hardware Testing

For physical devices, often located in hostile environments

- Integrated circuits;

- Smartcards: e-passports, SIM cards, credit cards;

- Personal devices: cell phones, PDAs;

- Embedded systems

    - Card readers, digital tachographs, alarm systems, electricity meters;

- Network devices ;

- Devices using ASICs, FPGAs or on-chip cryptographic functions.

Hardware Testing
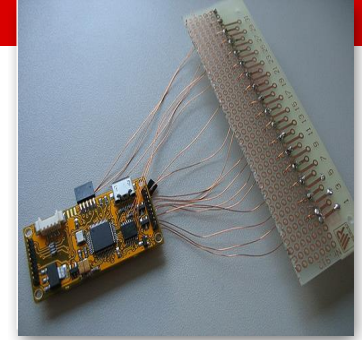
Our capabailities for hardware security testing include:

- Low Tech/Environmental Tests

- Moderate Tech/Passive and Probe Tests

- High Tech/Energy Tests

- Enclosure hardening

- Tamper evidence, tamper detection, tamper response testing and consulting

- Embedded software architecture security design review and source code review

- Consulting on Monolithic kernels such as Embedded Linux and Microsoft CE

- Protocol Analysis including proprietary network protocols and their network interfaces

- Cryptographic testing for ASICs and software implementations of algorithms

- Electromagnetic shield testing

Consulting

- Consulting associated with a Conformance testing project
  - Physical Security
  - Producing the Security Policy in conjunction with your key security and product architects
    - a timely and well-written SP can save weeks from the schedule and avoid costly overruns and errors
  - Support in providing the evidence needed
    - we minimize the evidence to the required minimum
    - we do NOT recommend producing any unneeded documentation
  - Support in producing the right test cases

Corporate Certification Strategy

- For companies where formal certification of products is a key marketing or customer requirement, atsec assists with

  – Determining the strategy for gaining and maintaining compliance for a variety of certifications including Common Criteria and FIPS 140-2

  – Synchronizing certification and re-certification with the product release cycle

  – Helping customers develop efficient development processes for one or more products saving money and time.

Commitment to Quality

- atsec ensures all internal processes are certified with the leading international standards

  - ISO 9001 for quality

    - ensures ALL internal business processes meet recognized standards, mature and improve.

    - covers everything from back-office processes to "lessons learned"

  - ISO/IEC 27001 for information security

    - ensures that information and IP entrusted to us stays safe at all time

  - ISO 17025 for laboratory services

    - ensures our formal laboratory procedures are world-class

Why do business with atsec?

- atsec **delivers** results **on time** and **at a fair price**

- atsec provides unique synergies:

  - Combined Common Criteria and FIPS 140-2 (or other) testing

  - Maximizes reuse of evidence while minimizing the time and costs

- atsec has global reach

- atsec employs experts with internationally-recognized track records

- atsec leads the industry

  - Contributing to development of standards

  - Advising schemes and programs about the state-of-the-art for information security

Find out much more at www.atsec.com