



atsec information security Common Criteria Services

CC laboratory managers

Who are we?



atsec information security has been involved with Common Criteria since the Company was founded in 2000

- atsec staff have decades of Common Criteria, ITSEC, TCSEC and related criteria schemes
- Accredited Common Criteria laboratories in
 - Germany, Sweden and the U.S.
- Over 100 Common Criteria certificates completed
- Formally trained and certified evaluators
- Recognized as leaders helping developing the standards and supporting the community
- A large portfolio of challenging evaluations

Experience



atsec has successfully performed over 100 CC evaluations of different types of IT security products.

-
- **operating systems (including Red Hat and SUSE Linux, AIX and z/OS)**
 - **database management systems (including Oracle and IBM DB2)**
 - **firewall systems**
 - **cryptographic components**
 - **printer controllers**
 - **logical partitioning systems**
 - **virtualization technology**
 - **access management systems**
 - **directory server systems**
 - **identity management systems**
 - **PKI infrastructure systems**
 - **administrative support and policy**
 - **enforcement systems**
-

The CCRA

- With the establishment of Common Criteria a mutual recognition agreement was necessary to allow the different governments to accept evaluation results from other nations in the scheme.
 - The initial 7 members formed the Common Criteria Recognition Agreement or “CCRA”
- 17 nations signed to show that they will accept the certificates from other nations **and** issue CC certificates
- 8 nations signed to show that they will accept the certificates from other nations even though they do not issue certificates.
- The CCRA establishes international recognition only up to a commercial level evaluation assurance level EAL2 or to an endorsed cPP.



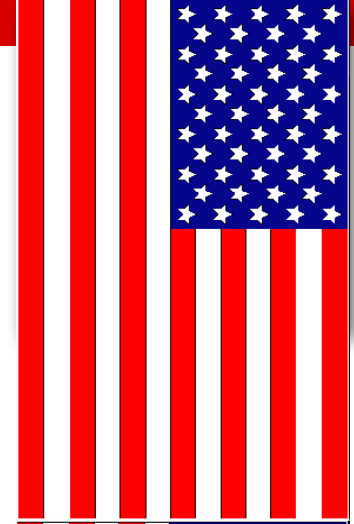
***Certificate
Producers***

***Certificate
Consumers***

***A cPP is a
“collaborative
Protection
Profile”***

The US Scheme (CCEVS)

- U.S. National Information Assurance Partnership's (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS)
- One of the original 7 nations developing the CC
- Makes key policies requiring Common Criteria certification of Commercial Off The Shelf Products that are used in the U.S. Federal arena
- Web URL: <https://www.niap-ccevs.org>



atsec offers evaluation with the U.S. national scheme



The German Scheme (BSI)

- BSI “Bundesamt für Sicherheit in der informationstechnik“
- One of the original 7 nations developing the CC
- The goal is to promote IT security in Germany
- Central IT security service provider for the German government
- Is one of the ten members of the SOGIS arrangement

- Web URL:
https://www.bsi.bund.de/EN/Topics/Certification/certification_no_de.html

atsec offers evaluation with the German national scheme



The Swedish Scheme (CSEC)

- Swedish CC scheme, Sveriges Certifieringsorgan för IT-säkerhet (CSEC) operated by FMV
- Joined the CCRA as a certificate producing nation in 2007
- Is one of the ten members of SOGIS
- Web URL:
<http://fmv.se/en/Our-activities/CSEC---The-Swedish-Certification-Body-for-IT-Security/>

atsec offers evaluation with the Swedish national scheme

Why Choice Matters

- Even though the criteria standards and the CCRA are common, national scheme differences exist:
- The CCRA establishes recognition by 25 CCRA signatories up to a commercial level evaluation assurance level, EAL2
- SOGIS establishes between most European schemes, recognition up to EAL 7 for some technologies
- National policies vary for acceptance of products into a validation scheme
- Available validation resource varies in different national schemes: Validation times and charges vary
- Experience and expertise in particular technology areas vary
- Some commercial companies naturally establish relationships with particular national schemes



CCRA=
Common
Criteria
Recognition
Arrangement

SOGIS=
Senior
Officials
Group -
Information
Systems
Security

atsec's Common Criteria Services

- Readiness Assessment
- Training
- Evaluation available in 3 national schemes
 - US Approved PPs
 - ST only (Germany & Sweden only) up to EAL7
 - PP (Germany & Sweden only) up to EAL7
 - cPP (in endorsing nations)
- Consulting
 - ST development
 - PP development
 - Others
- Corporate global certification strategy
- National scheme development



ST=
Security
Target

PP=
Protection
Profile

cPP =
Collaborati
ve
Protection
Profile

Readiness Assessment



A readiness assessment helps

- Establish a certification strategy
- Establish boundaries of the product for CC evaluations. (Defines the TOE)
- Discover any gaps and discuss remediation
- Introduce the developer and evaluator teams, establishing good rapport
- Allow atsec to estimate costs and hence offer a fair fixed price
- Perform basic Common Criteria training

TOE=
Target of
Evaluation

Typically 2 days duration. Costs may be recovered from the full evaluation project.

Training



We offer training for Common Criteria

- Introductory workshop suitable for business and commercial level managers (2 hrs- ½ day)
- Developer training suitable for key development staff involved in Common Criteria projects (5 days)
- Workshops on information security topics for certain technologies
- Conversion workshops for key development staff when the Common Criteria version changes
- Evaluator training for laboratory staff
- Validator training for national schemes

Evaluation

- atsec has evaluated over 100 products
- Evaluation projects of new products typically last
 - 9 months for an average amount of security functionality. Longer for more complex TOEs
 - 6 months for a typical re-evaluation projectsOur evaluations include many complex products
- Conformance evaluation resulting in a certificate issued either by
 - U.S. national scheme
 - German national scheme
 - Sweden national scheme



TOE=
Target of
Evaluation



The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). 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: IBM Global Security Kit V7.0.4.11
Evaluation Platform: AIX 4.3.3, 5.1, 5.2, 5.3; Solaris 7, 8, 9, 10; HP-UX 11, 11i, 11V2, 11V3; Windows NT, XP, 2000, 2003; Vista; RHEL 2.1, 3, 4, 5; SLES 8, 9, 10 (for specific versions and patch levels see Section 2.4.3 in Security Target)

CCL: atsec information security corporation
Validation Report Number: CCEVS-VR-07-0039
Date Issued: 2 August 2007
Assurance Level: EAL 4
Protection Profile Identifier: None

Original Signed By
Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Original Signed By
Information Assurance Director
National Security Agency

Consulting

Consulting associated with a Common Criteria project is typically related to

- Producing the ST in conjunction with your security and product architects. A timely and well written ST can save weeks from the schedule and avoid costly overruns and errors.
- Support in providing the evidence needed. Including design information and assurance information. atsec keeps to the evidence required and does not recommend producing unneeded documentation.
- Support in producing the right test cases.
- Support with predictive assurance.



ST=
Security
Target

SECURITY TARGET FOR PRISM ON THE IBM SYSTEM z10 EC

Common Criteria for Information Technology
Security Evaluation

Public Version
of the
Security Target for
PRISM for the
IBM System z10 EC™

Version 7.7.2
October 23, 2008

This Security Target was developed for the evaluation of the Processor Resource/Systems Manager™ (PRISM™) for the IBM System z10 EC platform according to the Common Criteria level EAL5. The intention of this Security Target is also to show the compliance of PRISM with the requirements identified in the Common Criteria for those functions identified in this document.

PRISM Security Target

i

October 23, 2008



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.

National Scheme Development



atsec has so much experience with Common Criteria that we are frequently asked to assist with:

- National scheme shadowing (One of the processes as part of the CCRA ensuring scheme conformity)
- Developing various national certification schemes as nations seek to enter the CCRA
- Training national scheme validators in the techniques used in evaluating (and hence validating) complex technologies such as operating systems

atsec's Quality



atsec takes care to ensure that all of our processes are certified as compliant with the leading International standards

- **ISO 9001 for quality**

- Helping us ensure that ALL of our business processes meet recognized standards, mature and improve. From the back office processes to “lessons learned”

- **ISO/IEC 27001 for our information security**

- Helping us ensure that the information and I.P. entrusted to us stays safe

- **ISO 17025 for our laboratory services**

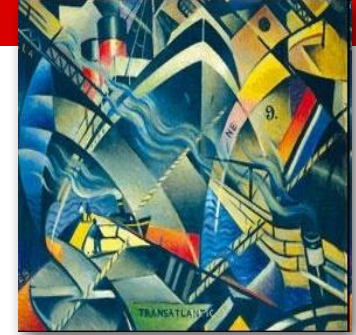
- Helping us ensure that our formal laboratory procedures are world class



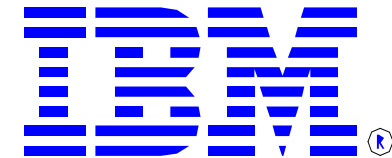
atsec's Differentiators

- **Experience:** With over 100 evaluations completed successfully atsec's staff are world renowned for competence in their field and atsec has an unsurpassed reputation for quality
- **Synergies:** If also need other testing such as FIPS 140-2 atsec can provide both
 - atsec maximizes reuse of evidence and timing of testing ensuring cost savings
- **Expertise:** atsec lead the information security industry, contributing to international standards development and advising schemes and programs about the state of the art of information security
- **International:** atsec can offer evaluation under three schemes and can use staff from Europe and the U.S.

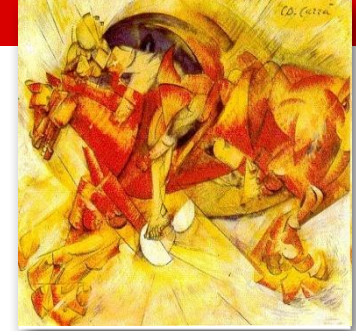
Confidence in atsec



We offer gratitude to the many companies, large and small, who help atsec thrive and trust us with their Common Criteria needs...



Find out much more at www.atsec.com



atsec
the information security provider

home | sitemap | blog

- Services
- Company
- News & Events
- Resources
- Contact

Deutsch | 汉语

atsec information security

Austin, Texas, Munich, Germany, Stockholm, Sweden, Beijing, China

News

IT Security Companies to Host Protection Profile Developer Workshop
2011-01-13

Parallel to this year's RSA conference in San Francisco, atsec information security and a group of IT security companies

Welcome to atsec. We are a United States Government accredited laboratory for testing information assurance (IA) and IA-enabled commercial off the shelf (COTS) information technology.

Whether you need affordable testing, consulting, or compliance, atsec can help. Take a look at the wide range of IT security services we offer, or browse through our IT security resources to learn more about the multiple standards we work with.

atsec's thought leadership at
<http://atsec-information-security.blogspot.com/>

atsec IT security blog

NEWS ABOUT COMMON CRITERIA, FIPS 140-2, NASPO AND OTHER IT SECURITY TOPICS

