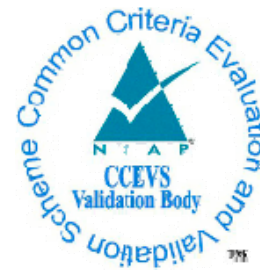




atsec information security Common Criteria Services



Ken Hake

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.
 - Approaching 90 Common Criteria certificates
 - Formally certified evaluators
 - Recognized as leaders developing the standards
 - A large portfolio of challenging evaluations

Experience



- atsec has successfully performed more than 85 Common Criteria 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**

About Common Criteria

- It's a security certification for IT products
- Mandated in the US
 - See <http://www.niap-ccevs.org/cc-scheme/> for the latest details
 - NSTISSP No. 11
 - DoDD 8500.01E, and DoDI 8500.2
- Joint Interoperability Test Command
 - CC is one of the certifications
 - FIPS
 - STIGS



About Common Criteria



- Since the use of IT became widespread, the establishment of criteria for assessing the security of complex IT products continues to be the goal of many nations:
 - US: The Orange book, TCSEC, was published in 1983 and established security evaluation criteria
 - The Canadians followed with their own criteria, CTCPEC in 1993
 - The German criteria were the first to separate security functionality and security assurance
 - The UK, France, Germany and the Netherlands criteria, ITSEC, introduced the “Security Target”
 - The Federal criteria introduced the “Protection Profile”
 - The first “Common Criteria in 1996. V 3.2 in 2009

National Schemes for certification

- 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”. They performed evaluations and issued certificates.
- Some nations signed to show that they will accept the certificates from other nations even though they do not formally perform evaluations themselves.



***Certificate
Producers***

***Certificate
Consumers***

CCRA in 2011

Certificate Producers (and consumers)



Australia



Canada



France



Germany



Italy



Japan



Netherlands



Norway



New Zealand



Republic of Korea



Spain



Sweden



Turkey



United Kingdom



United States

CCRA in 2011: Certificate Consumers



Austria



Czech Republic



Denmark



Finland



Greece



Hungary



India



Pakistan



Israel



Malaysia



Republic of
Singapore

Why Choice Matters

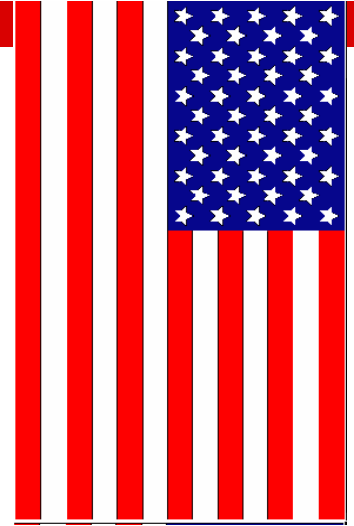
- Even though the criteria and CCRA are common, national scheme differences exist:
- The CCRA establishes recognition only up to a commercial level evaluation assurance level, EAL4
- National policies vary for acceptance of products into the validation scheme and at EALs 5-7
- Available validation resource 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

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: <http://www.niap-ccevs.org/cc-scheme/>



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
- Web URL:
<http://www.bsi.bund.de/english/index.htm>



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
- Web URL:
<http://www.fmv.se/WmTemplates/Page.aspx?id=824>



atsec offers evaluation with the Swedish national scheme



atsec's Common Criteria Services



- Readiness Assessment
- Training
- Evaluation in 3 schemes
 - IT products
- Consulting
 - ST development
 - PP development
 - Others
- Corporate global certification strategy
- National scheme development

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



TOE=
Target of
Evaluation

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 85 products
- Evaluation 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



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
PR/SM 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™ (PR/SM™) for the IBM System z10 EC platforms according to the Common Criteria level EAL5. The intention of this Security Target is also to show the compliance of PR/SM with the requirements identified in the Common Criteria for those functions identified in this document.

PRISM Security Target

October 23, 2008

Corporate Global 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



Differentiators

- Synergies: If you need both Common Criteria and FIPS 140-2 (or other) testing
 - atsec maximizes reuse of evidence and timing of testing ensuring cost savings
- atsec's staff are world renowned for competence in their field and atsec has an unsurpassed reputation for quality
- 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
- atsec has global reach

Confidence in atsec



Doc Shanker, Certified Executive IT Architect, IBM Linux Technology Center

"...very impressed by the technical depth and professionalism of the atsec staff... atsec consultants have produced first-rate work on every project."

Charles Daniels, Systems Integration Environment Manager, US Marine Corps Systems Command

"As the customer, we were very pleased with atsec's approach, timely communication with the developer, and thoroughness of their evaluation of the PKIF v2 library. Our mission to enable application developers to efficiently use Public Key Infrastructures continues to benefit from the value added by the high quality of atsec's evaluation results."

Roman Drahtmueller, Security Architect, Novell/SUSE

"On behalf of Novell/SUSE, after more than 2 years of successful partnership with atsec, we are looking forward to the upcoming security evaluation projects for our products. It may be difficult to state that atsec as an evaluator is doing a great job, since that's what's expected before the background of the regulations of the Common Criteria.

However, the mature experience, the outstanding expertise and the proficiency in organization and management shown by atsec's evaluators and security experts make an evaluation project an experience by far beyond a security evaluation for the benefit of our customers: Exciting, fascinating, enjoyable."





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...

