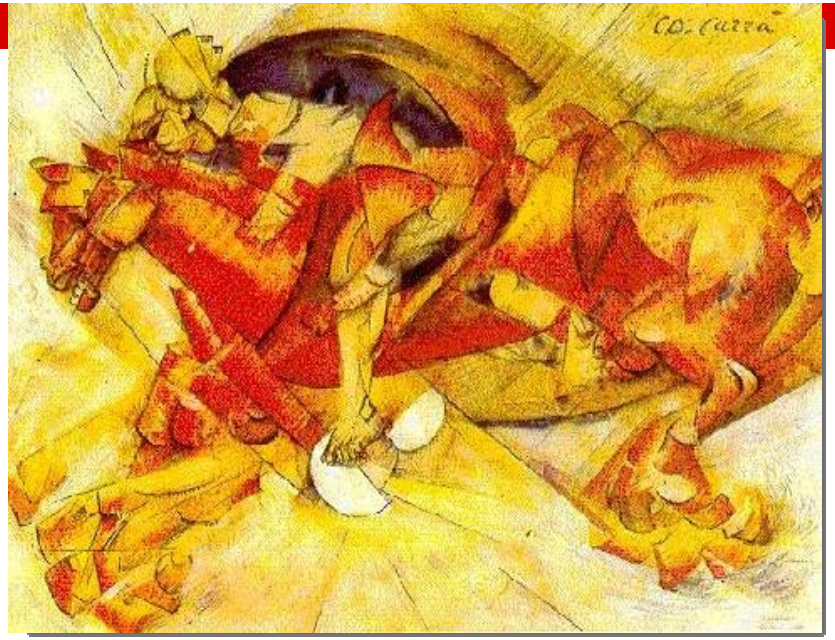
the information security provider



Becoming a CNAS Laboratory

Yi Mao, Ph.D., CISSP
atsec information security corporation

yi@atsec.com

Shi Cao, Director
Laboratory Assessment Department
China National Accreditation Service for Conformity Assessment

caos@cnas.org.cn

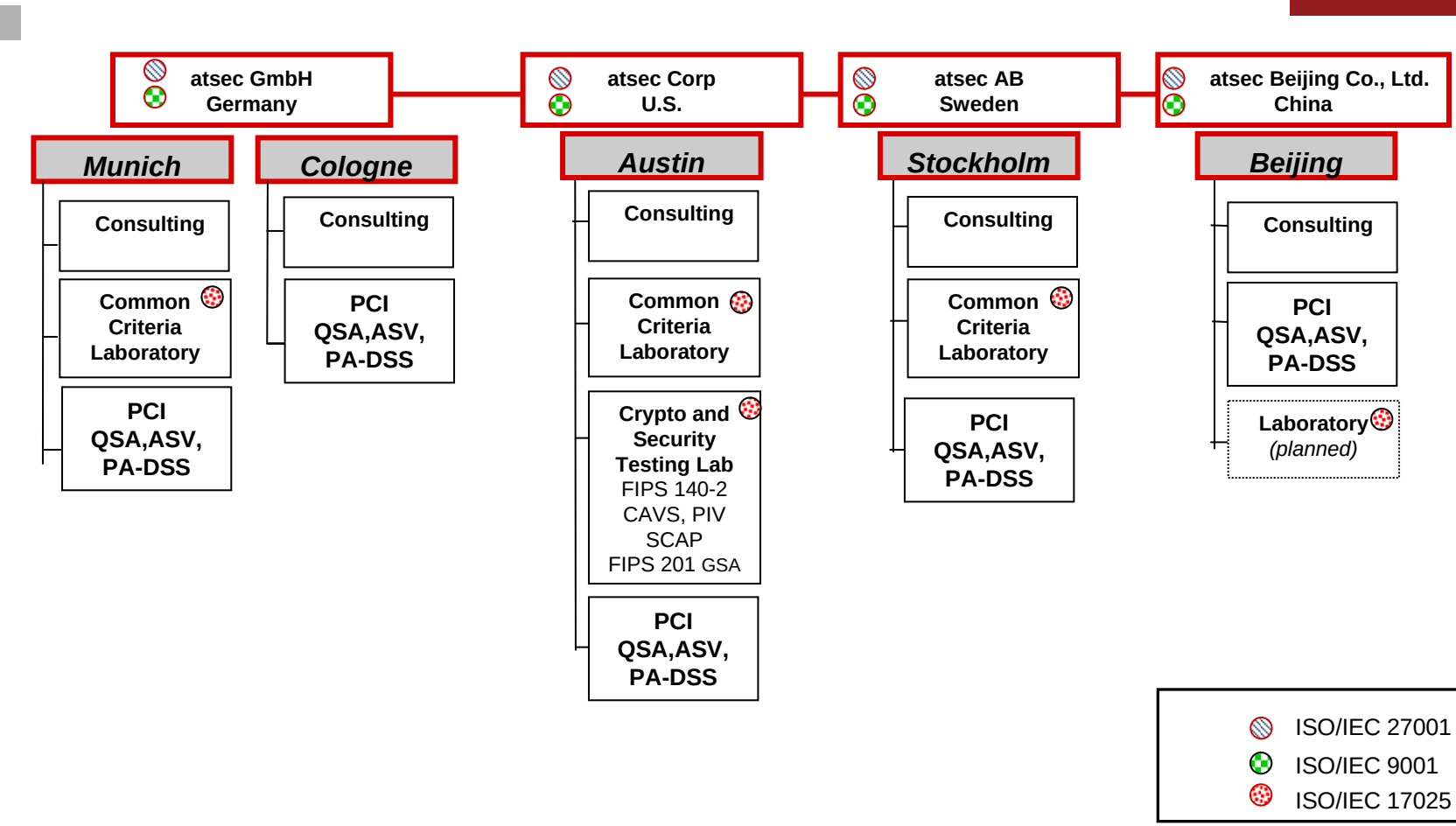
Yan Liu, Director
atsec China

yan@atsec.com

Agenda

- Introduction to atsec and atsec China
- Motivation for becoming a CNAS lab
- Feasibility analysis for becoming a CNAS lab
- Introduction to CNAS
- Difficulties encountered
- CNAS conclusions
- What atsec China can and cannot do
- A mutually-beneficial experience
- Acknowledgements

Introduction to atsec



Introduction to atsec – Some of Our Global Customers

IBM

redhat

DELL

IEEE

Microsoft

vodafone

hp

redhat

ORACLE

Honeywell

CRAY THE SUPERCOMPUTER COMPANY

Introduction to atsec China – Some of Our Chinese Customers

HUAWEI H3C ITolP解决方案专家 ZTE中兴 清华同方 TSINGHUA TONGFANG 中兴集成电路 国民技术 nationz technologies 华大电子

SYNO CHIP 杭州晟元芯片技术有限公司 Synochip Corporation

Shanghai Huahong Integrated Circuit Co.,Ltd.

Neusoft

PCI部分客户 (Part of PCI related customers)

快钱 99BILL.com 易宝支付 YEEPAY.COM 绿色支付 快乐生活

billtobill NET REVENUE

oncard Payments China

首信易支付 PayEase

CUP DATA 银联数据服务有限公司 CHINA UNIONPAY DATA SERVICES CO., LTD

艺龙旅行网 eLong.com

freeborders Freedom without boundaries™

Euronet WORLDWIDE

Giesecke & Devrient Creating Confidence.

金邦达 GEMPLUS

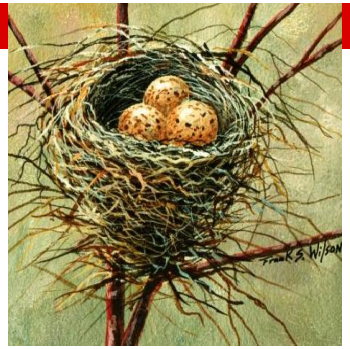
东信和平 EASTCOMPEACE

Milanoo.com

东信 EASTCOM

中国民生银行 CHINA MINSHENG BANKING CORP., LTD. 信用卡中心 Credit Card Center

Motivation for Becoming a CNAS Lab



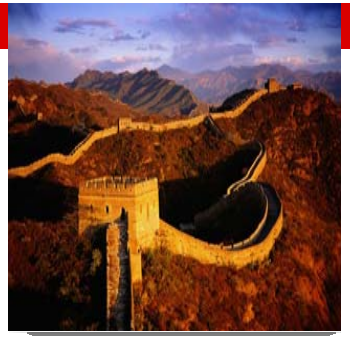
- atsec's determination to establish an independent, commercial, security lab in China is driven by our clients' needs:
  - Help our western clients achieve CC-equivalent certificates in China (and potentially, compliance to other Chinese standard)
  - Help our Chinese clients achieve CC certificates under CCRA
- atsec aims to bridge the gap between CCRA countries and China.
- atsec is passionate about contributing its professionalism to the worldwide IT security industry.
- atsec can contribute further to the global CC community by expanding atsec's international evaluation experience.

Feasibility Analysis for Becoming a CNAS Lab (1) -- atsec's Qualifications

- atsec is an accredited CC lab in:
  - the USA under the NIAP scheme
  - Germany under the BSI scheme
  - Sweden under the CSEC scheme

atsec's accreditation is dependant upon our being compliant with ISO/IEC 17025 and demonstrating proficiency in CC evaluations.

Feasibility Analysis for Becoming a CNAS Lab (2) -- atsec China's Qualifications



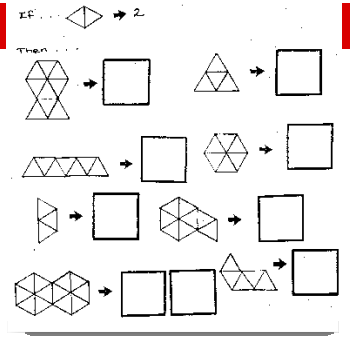
- atsec China is operated under the same Global Quality Management System (GQMS) shared by other atsec offices and proven to be ISO/IEC 17025 compliant through their CC lab accreditation.

  GQMS is structured in four layers: policies, procedures, templates and records. atsec offices share policies and procedures. atsec China may create their own work templates that are specific to the region and they are responsible to keep their work related records.

- atsec China is supported by atsec's global employee base which has expertise in the CC as well as broad experience in numerous other standards for IT security evaluation.

  atsec China leverages atsec's global CC expertise, but they do not have access to the customer data stored in other atsec offices. atsec keeps strict separation of the data storage that are specific to different atsec offices so that the integrity and intellectual property of our customer data are well protected.

Feasibility Analysis for Becoming a CNAS Lab (3) -- From Hypotheses to Conclusion



If:

- China uses ISO/IEC 17025 as lab accreditation criteria
- CC is an available standard in China for IT security evaluation

Then:

- it is possible for atsec China to gain lab accreditation for conducting CC-based evaluations

- Note: CC V2.3 was translated into Chinese and became a national standard “GB/T 18336.”
- Question: How is lab accreditation performed in China?

Intended Testing Scope of atsec China Lab

- GB/T 18336-2008 信息技术 安全技术 信息技术安全性评估准则
- ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security
  - Part1: Introduction and general model
- ISO/IEC 15408-2:2008 Information technology – Security techniques – Evaluation criteria for IT security
  - Part2: Security functional components
- ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security
  - Part3: Security assurance components
- ISO/IEC 18045:2008 Information technology – Security techniques – Methodology for IT security evaluation

Introduction to CNAS (Chinese Web page)

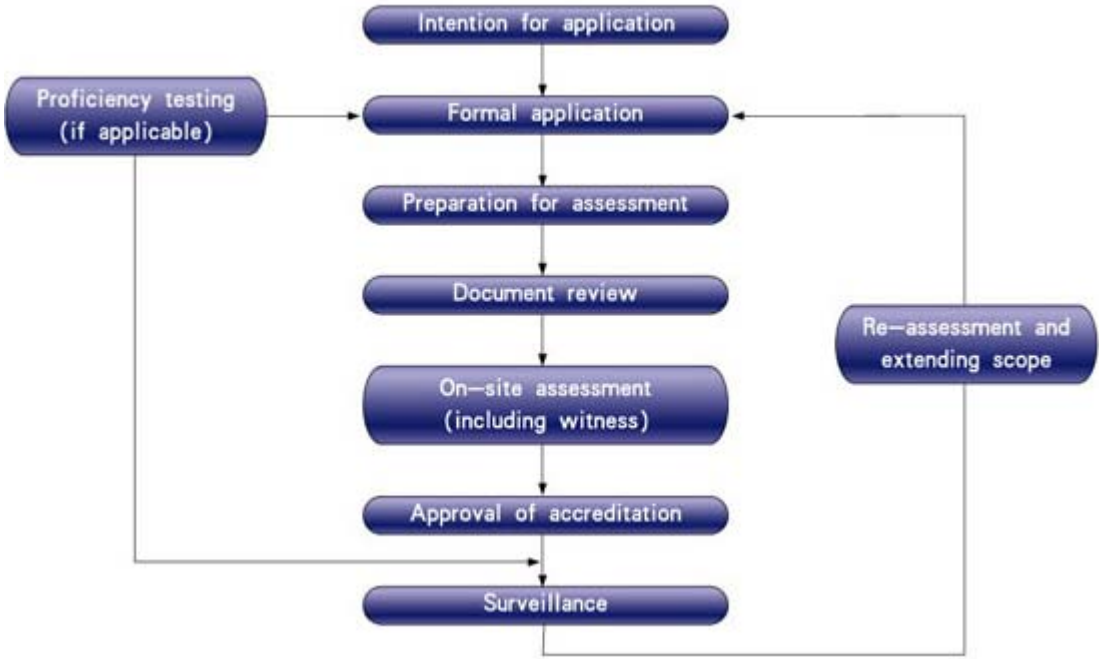
Introduction to CNAS (English Web page)

Introduction to CNAS (Continued)

- CNAS grants accreditation of:
  - A Certification body (based on ISO/IEC 17021 and 17024)
  - A Laboratory (based on ISO/IEC 17025)
  - An Inspection body (based on ISO/IEC 17020)
- CNAS lab accreditation is voluntary; however, it is often driven by various factors and becomes a demanding qualification:
  - Industry-specific requirements
  - Organization-specific requirements
  - Project-specific requirements
  - Marketing requirements
  - Leadership requirements

The CNAS Process for Lab Accreditation

- The CNAS lab accreditation generally goes through 3 main steps: application submission, document review, and on-site assessment. A typical accreditation process is shown below:



Risks Faced by CNAS

- In recent years, CNAS has received about 600 lab accreditation applications annually.
- CNAS must scrutinize each documented Quality Management System (QMS) against ISO/IEC 17025 at the documentation review stage, so that the CNAS manpower won't get wasted on on-site visits for applications that fail at the documentation review stage.
- CNAS must have well-trained personnel to differentiate a genuine QMS from a fake one by examining its documentation.
- There is a level of risk in accrediting a lab that may turn out to have quality issues.
- Risk is mitigated through a rigorous documentation review and strict on-site assessment.

The First Lab Candidate

- atsec China is the first applying lab that is:
  - independent
  - commercial
  - performing IT security evaluations

- CNAS has been extraordinarily attentive to the lab accreditation application for this first commercial, independent lab in the area of IT security evaluation.

Difficulties Encountered During Documentation Review (1)

CC part 3 and GB/T 18336 (i.e., Assurance Components) cannot be included in the scope of accreditation of a Testing Lab because the CC part 3-related evaluation work is assigned to an Inspection Body to carry out.

Therefore, atsec China must be accredited both as a Testing Lab (conforming to ISO/IEC 17025) and an Inspection Body (conforming to ISO/IEC 17020).

Difficulties Encountered During Documentation Review (2)

- CNAS does not have a standard equivalent to NIST HB150-20 (Information Technology Security Testing: Common Criteria) that specifically tailors the ISO/IEC 17025 requirements towards being a CC-based IT Security Testing Lab. Therefore, the generic requirements from ISO/IEC 17025 on testing methodology, tools and equipment, calibration, and sampling etc., need to be re-interpreted in the context of IT security evaluations.

  (It may be that other schemes have similar limitations, and that the USA is unique in having HB 150-20.)

- CNAS does have guidance document on the Application of Laboratory Accreditation Criteria in the Field of IT Software Product Tests (i.e. CNAS-CL20). However, it is not written specifically for CC-based IT security testing labs; therefore, an appropriate interpretation of 17025 conformance in this particular context is still missing.

Difficulties Encountered During Documentation Review (3)

- atsec has a single, integrated QMS which addresses:
  - various standards including ISO/IEC 17025, ISO/IEC 27001 and ISO 9000
  - different geographically-located branches, including China, Germany, US, and Sweden offices.
  - various testing labs within atsec, including CCTL, CST, GSA, PIV, etc.

This QMS poses challenges to the CNAS assessors, who only need to look into the ISO/IEC 17025 compliance for atsec China lab.

Note: The above challenges are not unique to China. They have also been apparent to atsec's assessors.

Difficulties Encountered During Documentation Review (4)

atsec China has access to global atsec personnel to secure adequate and appropriate CC expertise. However, CNAS has concerns about the accountability of non-local personnel:

- How to audit lab activities of personal who are not located in the atsec China office?

Difficulties Encountered During On-site Assessment –- Mismatched Expectations (1)

atsec China's expectation:

- The QMS is functioning as documented
- atsec will show CNAS that we understand the CC and GB/T18336 and we know how to conduct a security evaluation based on CC or GB/T 18336
- atsec will conduct CC or CC-like evaluations once the lab accreditation is granted
- atsec is willing to take any available proficiency tests for the lab as well as for individual qualifications

Difficulties Encountered During On-site Assessment –- Mismatched Expectations (2)

CNAS' expectation:

- The QMS is functioning as documented
- As an applying lab, atsec must have done some lab work in the area in which it is applying for accreditation. Provide it to CNAS.
- Let CNAS witness atsec conduct an evaluation that atsec claims it can perform — right here, right now. CNAS will access your proficiency based on our real-time observation.

Note: This may not be unique to CNAS. Other schemes may hold that kind of expectation, too.

atsec China's First CC Project

- A friendly CC client agreed to allow atsec China to conduct a sample CC evaluation on one of its products.
- atsec signed an NDA with our CC client and obtained all necessary design documentation.
- atsec wrote an ST, including SFRs in FAU, FCS, FDP, FIA, and FMT classes.
- atsec completed the draft reports for ASE, ADV, AGD, ALC, ATE (a separate report for IND), AVA, and ETR.
- atsec conducted an on-site visit at our client facility for source code review and some requirements covered in ALC and ATE.

CNAS Verifies CC Reports

- CNAS reviewed the:
  - ST
  - evaluation reports
- CNAS provided feedback for improvement
- CNAS witnessed the on-site visit conducted by the atsec China team at the CC client facility.

CNAS' Conclusions (1) — ISO/IEC 17025 Compliance

- atsec China had some non-conformities in showing the records to prove that the QMS is followed in the daily lab work. These need to be addressed within two months and the changes made and/or the records updated must be reported back to CNAS.

- atsec China should localize the QMS, particularly for the China lab. All of the QMS documentation should eventually be translated into the Chinese language.

CNAS' Conclusions (2) — Lab Testing Scope

- CNAS will consider including the CC part 3 and GB/T 18336 within the lab testing scope, provided that atsec China can provide a convincing argument that CC part 2 and part 3 consist of one integral standard and hence cannot be isolated from each other. atsec China must also provide supporting evidence that CCRA countries do not require ISO/IEC 17020 conformance to accredit CC labs.

- CNAS confirms that atsec China has a good knowledge of CC through verbal interviews performed. However, the accredited testing scope must be determined by the SFRs (specified in the sample CC project) and the SARs (observed during the on-site assessment).

- During the annual surveillance audit, the accredited scope can be extended according to the CC and CC-like projects that atsec China will have completed by then.

Post-Assessment Discussions

- atsec can help to promote CC awareness in China.
- atsec can contribute to improving the lab accreditation criteria in the area of IT security evaluations.
- CNAS could consider monitoring the progress of a sample or real CC/CC-like project in a longer time frame (e.g. six months to a year).
- CNAS could consider waiving the requirement of observing the applying lab conduct test at a client's facility because the lab's client is not obligated to support this activity.
- CNAS could consider defining the scope of an applying lab's testing capability in a more general terms, such as CC EAL2 or CC EAL 4; rather than specifying the individual SFRs and SARs in terms of their class, family, and component.

What atsec China Can Do

- atsec China lab can write CC (based on ISO/IEC 15408) or CC-like (based on GB/T 18336) evaluation reports.

- The more reports atsec China completes, the more experience it gains, which will help to extend the test scope in two dimensions by including more SFRs and SARs.

What atsec China Cannot Do

- atsec China is not yet positioned to assist our clients with obtaining CC-like certificates.
- A government-run Chinese lab ITSEC used to issue CC-like certificates to IT products. Their certified products can be found at: http://www.itsec.gov.cn/cpyzcgg/cpcpgg/index.htm. Now, they can only provide evaluation reports just like atsec China.
- China Information Security Certification Center (ISCCC) is the authorized governmental agency that certifies IT products based on national standards other than GB/T 18336, such as:
  - GB/T 20272-2006 for Secure Operating Systems
  - GB/T 20281-2006 for Firewalls
  - GB/T 21028-2007 for Servers
  - GB/T 20276-2006 for Smartcard embedded software
  - etc.

A Mutually-Beneficial Experience (1)

- CNAS is extremely supportive and helpful.
- CNAS has taken on the challenge, including the language barrier, to carefully review and comment on atsec's global QMS.
- CNAS clearly explained their policy and accreditation process in great detail for justification.
- CNAS is yet very open to understanding atsec's lab accreditation experiences with BSI, NIAP, and CSEC.
- CNAS listened to atsec's explanations of the CC with great patience.
- CNAS is willing to improve their accreditation framework so it can work better for IT security evaluation labs.

A Mutually-Beneficial Experience (2)

- atsec China will follow CNAS' valuable advice to localize our QMS, integrate it into our daily work, and keep maintaining a high standard for the QMS.

Acknowledgements

- CNAS team (lead by Mr. Shi Cao)
  - Ms. Yansheng Cheng (documentation reviewer)
  - Ms. Chang Liu (technical reviewer and on-site assessment coordinator)
  - Ms. Yaoxi Chen (lead auditor for on-site assessment)
  - Dr. Hui Liu (on-site auditor)
  - Dr. Jian Gu (on-site auditor)
- atsec management team
- atsec China team (lead by Mr. Yan Liu)
- CC project sponsor -- Pierson team (lead by Mr. Frank Psaila)

References

- CNAS-CL01:2006 检测和校准实验室能力认可准则
  （ISO/IEC 17025：2005） Accreditation Criteria for the Laboratories
  http://www.cnas.org.cn/extra/col23/1153719823.pdf
- ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories
  http://www.iso.org/iso/catalogue_detail.htm?csnumber=39883
- CNAS-CL20: 2006 检测和校准实验室能力认可准则在信息技术软件产品检测领域的应用说明 Guidance on the Application of Laboratory Accreditation Criteria in the Field of IT Software Product Tests
  http://www.cnas.org.cn/extra/col23/1181021341.pdf
- NIST HB150-20 :2005 INFORMATION TECHNOLOGY SECURITY TESTING: COMMON CRITERIA
  http://www.nist.gov/ts/ssd/nvlap/upload/NIST-HB-150-20-2005-1.pdf
- ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security (CC v3.1)
- ISO/IEC 18045: 2008 Information technology -- Security techniques -- Methodology for IT security evaluation (CEM)
- GB/T 18336: 2008 信息技术安全技术信息技术安全性评估准则 (CC v2.3)
- atsec white paper on scheme differences:
  http://www.atsec.com/downloads/documents/Scheme_diffs_09-04-29-2.pdf