

atsec's sole focus has always been IT security - and knowing the business is one of our company's principles. From constant training to professional exchange with industry peers we do our best to stay on top of IT security developments.

In this newsletter we will share some thoughts on atsec's involvement in the international IT security standards community. From the company's early days we have been active in shaping the development of existing and new standards and will continue to do so in the future.

An important part of doing business in the area of IT security business is meeting the requirements put forth by various government and commercial organizations. For example, our offices around the world are ISO/IEC 27001 and ISO 9001 certified. We know the auditing and compliance business from both sides of the aisle. For a list of our accreditations and certificates, please take a look at: <http://www.atsec.com/us/atsec-iso-iec-9001-27001-certificates.html>

atsec is working hard in the Open Group Trusted Technology Forum. Here we support the consensus development of the "Open Trusted Technology Provider Framework" (O-TTPF) and join industry leaders striving to codify the best practices for supply chain security relevant to Commercial Off the Shelf Products. For more information, please visit <http://www.opengroup.org/ttf/>

We are also working closely with the North American Security Products Organization - NASPO, as ANSI SA-2008 undergoes review. ANSI SA-2008 is a security assurance standard used by organizations, both inside and outside of the U.S. An organization's compliance to ANSI SA-2008 demonstrates a secure operation, as well as the capacity to classify and officially certify themselves, through a NASPO or commercial audit, and the ability to deliver either a high, medium, or basic level of security assurance. More information is available at www.naspo.info

Finally, we would like to mention our participation in several upcoming IT security conferences around the world, as well as our training events regarding FIPS 140-2 and Physical Security in the coming weeks.

How can we help you?

Regards,

Andreas Fabis
Marketing Director

Recent news in short:

- IBM's® z/OS® Version 1 R. 12 System SSL Cryptographic Module receives FIPS 140-2 certification
- Steve Weingart to speak at the Non-Invasive Attack Testing Workshop in Nara, Japan
- atsec offers FIPS 140-2 and Physical Security Workshops in Austin and Stockholm
- atsec information security provides PCI training in Shanghai
- atsec information security completes the CMVP testing for two ZTE modules
- atsec to present five papers at the 12th ICCS Conference in Malaysia
- atsec information security at PCI Security Standards Council Community Meeting - Scottsdale, AZ

More news on our website:

www.atsec.com

Did you know atsec has a security blog?

Follow our consultants' thoughts and musings at: <http://atsec-information-security.blogspot.com>.

Also join us on Facebook and Twitter (@atsecitsecurity).

Common Criteria (ISO/IEC 15408) ■ FIPS 140-2 ■ CAVS ■ SCAP ■ NPIVP ■ GSA ■ FIPS 201 ■ NASPO ■ PCI QSA ■ PCI ASV ■ PCI PA-QSA ■ ISO/IEC 27001 ■ SOX and Euro-SOX ■ FISMA ■ HIPAA ■ VTDR ■ Embedded Systems ■ Hardware Security ■ Testing and Analysis ■ Penetration Testing ■ U.S. Export Control for Cryptography

Standards

Love them or hate them, standards, technical specifications, and associated guidelines are something that atsec and its customers are involved with on a daily basis. But why would a small company like atsec get deeply involved with standards development?



After all, it's a huge investment for atsec once you consider the fees to join the standards organization, the travel expenses to travel to meetings in far away locations - or conversely, the cost to host meetings at our location, and in some cases we even have to pay a fee to attend the meetings. We donate a lot of our consultants' precious time to work on the development of the standards; a process that involves often daily and seemingly endless conference calls, days of reading and commenting on a plethora of documents, and time spent acting as editors to coordinate with large groups of people representing disparate organizations to help guide them to a consensus. The work involves little recognition for the effort and, at least for atsec, no outside financial support. Once a standard is published, if we want to use it in our business, then we even have to pay to buy the standard that we helped write!

What does this bring to atsec?

Working on standards development means that we gain a high level of relevant expertise and can consult clients on how to apply and implement such standards. It means that we understand not just what the content of the standard is, but **why** it is written that way. atsec was there when the world's technical experts had a five-hour discussion on why something had



to be "just so" in the standard. We know not only **what** and **why** something was written in a particular way (or, in fact, left out completely), but actually **what was intended** when it was written. The background discussions, the various con-

tributions, the different opinions, and even an understanding of the vested interests expressed give us insights that many of our competitors lack.

Over the years, we have been heavily involved with the development of standards in formal standards organizations such as ANSI, ISO, and industry-led consortia such as The Open Group. We have actively supported organizations such as the IEEE, NIST, and PCI SSC in their development efforts by providing comments and other contributions.

In ISO, we sponsored employees as editors for ISO/IEC 15446, Guide for the production of Protection Profiles and Security Targets; ISO/IEC 15408-1, the Evaluation criteria for IT security - Part 1, ISO/IEC 15443, A framework for IT security assurance, and for ISO/IEC 27002, the code of practice for information security management. We have been rapporteurs for study periods on Systems Evaluation and also for Secure system engineering principles and techniques. In the Open Group, we are contributing to The Open Trusted Technology Provider Framework and in CEN we provided a co-author for CWA 14167-2 "Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP."

From Chinese walls to the Chinese wall, sometimes in the shadow of the Chinese Wall



Our involvement with developing such a broad range of standards and guidance also helps us learn from our industry colleagues, many of whom are also our customers. Of course, we have an unrivalled opportunity to learn a lot technically - after all, we get to rub shoulders with the world's recognized experts in diverse topics from the specifics of a particular security model to the nuances and problems associated with a global supply chain. The standards groups we are a part of focus on all things security, including the specification of cryptographic primitives, protocols, applications, orga-

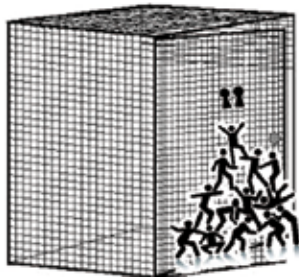
nizational processes, and governance. We keep these issues in mind as we take a hard look at the best way to evaluate or test real-world implementations of security-related technologies and processes.

There is a supply chain for security assurance, as well. atsec works a lot with vendors of IT products. One thing that we are constantly trying to keep up with is the needs of their customers – the end users of those IT products. If we understand the security assurance that they need, then we can serve our customers more effectively. While we have several ways of staying abreast of the latest trends, the standards forums provide one place where we can hear the vendor's most pressing concerns and issues directly.

What does atsec bring to the standards community?

A deep and varied experience with the security issues faced in the real world is one of the things that atsec brings to the standards community. Not all standards are straightforward technical specifications such as those described in ISO/IEC 18033 "Encryption algorithms." atsec is fortunate to have a diverse customer base that includes not only those from the select Fortune 100 companies, but also many small and medium-sized companies. We work with them on their product security, on the security of their organizations, and on meeting the mandatory requirements of the markets they are in. We help them not only with meeting certification or qualifications required in their markets, but also to provide them with security expertise that is otherwise hard to find.

Experience with the assessment, evaluation, and conformance testing activities that are the needed extension of the standards and technical specifications is a highly-specialized skill. Even when technology experts craft the standards, they often are not experts in the corresponding assessment that must be performed against those standards. We often see requirements drafted that seem an obvious necessity to those who develop the technology, but in fact may be difficult to assess as intended.



"If possible, arrange for the storage cages to be only opened by the simultaneous application of two keys or biometric indentifiers to two electronic locks that are physically beyond the reach of a single individual."

The old adage: "there is more than one way to skin a cat," is true in the standards world, and, at least for process and organizational-level standards, an important attribute of a successful standard is consideration of all the potential users; the large and small, global and local, innovative, and mass-producers. Even with some lower-level technology standards it's important to remember that the technology will evolve, and therefore consideration should be given to consider ways to embrace that eventual change.

atsec is well known for its abilities to take on complex and challenging Common Criteria evaluations as well as for conformance testing for FIPS 140-2, but we also work with compliance to standards demanded by legislation, regulation, and procurement norms such as those related to PCI, NASPO, FISMA, and ISO/IEC 27001. Together, our more senior consultants have accumulated what totals up to centuries of experience, and have found that many of the contemporary problems being addressed are not new. atsec helps customers from just about every industry segment from agriculture to utilities. We work with small innovative research & development companies with newly-developed technologies that do not always fit exactly to the requirements of published standards and specifications. We also have several projects helping organizations give demanded assurance to customers (even when recognized standards have not yet been defined). We feel that it is important to bring our experience to the standards arena. With such practical experience, we can contribute not only to the definition of new documents, but also to revisions of existing ones, as our consultants continue to gain experience that keeps us on the cusp of new and evolving technologies and industry know-how.

FREE AS IN BEER!

ISO publish some standards for free.

<http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>

atsec has contributed to many standards and industry bodies over the years including:

- AFCEA, BITKOM
- CAST (Competence Center for Applied Security Technology)
- CEN
- EMVCo. IEEE
- INCITS DAPS 38
- INCITS CS1 Cyber Security (US ISO/IEC JTC 1/SC27 Shadow)
- NASPO (North American Security Products Organization)
- NERC (North American Electric Reliability Corporation)
- PCI SSC
- The Open Group Trusted Technology Forum
- SHARE, Smart Card Alliance
- TeleTruT

IBM's® z/OS® Version 1 R. 12 System SSL Cryptographic Module Receives FIPS 140-2 Certification

Austin, TX – IBM's® z/OS® Version 1 R. 12 System SSL Cryptographic Module recently received FIPS 140-2 Level 1 certification. The successful certification is listed on the National Institute of Standards and Technology's (NIST) website (<http://csrc.nist.gov/groups/STM/cmvp/validation.html>, certification number 1600).

The security of information assets is an ongoing problem of increasing importance for many companies in view of the constant rise of threats. IBM® z/OS® - one of the world's most advanced operating systems - has shown persistent commitment to their customers by providing solid means for securing valuable data: having undergone numerous Common Criteria evaluations at high assurance levels and corresponding FIPS 140-2 validations of the critical cryptographic components within.

Apostol Vassilev, CST laboratory manager for atsec, commented: "The System SSL module is a part of the foundation for all security services on the IBM z/OS v1 R12 in the context of advanced and unique technologies intended to improve the scalability, performance, and security of the platform. It combines software, hardware, and firmware within the cryptographic boundary on the z/OS architecture and delivers a high-level of cryptographic performance for the range of supported cryptographic services backed by the strong security assurances provided by the FIPS 140-2 standard. The validation of this version of the module demonstrates IBM's commitment to the development of advanced technology compliant with established standards for the benefit of their user community. It also shows the ability of the atsec CST lab to perform this challenging validation of

a fast-evolving module in its third validated edition within the bounds of the FIPS 140-2 standard."

MEET US AT THE CONFERENCE

Besides being heavily involved in national and international standards committees and industry groups, we also attend IT security conferences to stay on top of current developments in our field of expertise. Conferences also are a good way to connect with our current and future customers in a personal manner. If you attend any of the following conferences, we would like an opportunity to talk to you about your IT security, upcoming projects, and the ways we can help you meet your IT security testing, evaluation, compliance, or training needs:

- **IT-SA**
October 11 - 13, 2011 - Nürnberg, Germany
- **LASCON 2011**
October 28, 2011 - Austin, TX
- **MILCOM 2011**
November 7 - 10, 2011 - Baltimore, MD
- **ACSAC 2011**
December 5 - 9, 2011 - Orlando, FL
- **RSA 2012**
February 27 - March 3, 2012 - San Francisco, CA
- **SXSW Interactive**
March 9 - 13, 2012 - Austin, TX

For more information about the FIPS 140-2 standard, please visit our website at <http://www.atsec.com> and the NIST website at <http://www.nist.gov>.

UPCOMING TRAININGS

atsec offers both regularly scheduled and customized, on-demand education and training courses at our facility or on-site at your location. We have held country-specific trainings in Korea, Taiwan, Turkey, as well as other countries.

- **FIPS 140-2 Workshop** (1 day)
October 18, 2011 - Austin, TX
- **Physical Security Workshop** (1 day)
October 19, 2011 - Austin, TX

For more information, please visit <http://www.atsec.com/us/trainings.html>

CONTACT US

atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
USA

Phone: +1 512 615 7300
Telefax: +1 512 615 7301
Email: info@atsec.com