



Joint media release

Successful completion of a joint cryptographic project between EADS and A*STAR

- New cryptographic suites for telecommunication security applications
- Development of an innovative and secure electronic voting system
- A significant milestone for the long-term R&D partnership

Singapore, 26 November 2007 – The EADS Singapore Research and Technology Centre (Singapore) and A*STAR's Institute for Infocomm Research (Singapore) (I²R), are jointly announcing the successful completion of a cryptographic cooperation project in Singapore today.

Launched in October 2006, the key objectives of the cryptographic joint scientific cooperation project were to build and validate new cryptographic suites for telecommunication security applications and to develop a secure electronic voting system for protecting the privacy of ballots while allowing the summing up of the votes and evaluating the outcome.

Said Dr Ulrich Schnaut, COO of EADS Singapore Research and Technology Centre, "The results of this debut collaborative project between EADS and A*STAR marks a significant milestone for the long-term R&D partnership between our two organisations. To further develop our partnership, EADS and A*STAR are currently working on an overarching research collaboration framework agreement which would allow future projects to be launched without lengthy legal negotiations."

"This is I²R's first collaboration with EADS and we are pleased with the successful completion. It has proven, yet again, that our institute's crypto R&D expertise can be applied to meet industry needs," said Prof Lye Kin Mun, Deputy Executive Director (Industry) of I²R.

This joint project was led by Dr Bao Feng, Head of the Cryptography and Security Department of I²R in partnership with experts from EADS. Major scientific results from the joint project include:

- two innovative cryptographic block ciphers jointly designed and evaluated by both parties, for the use in secure mobile communicators,
- an in-depth analysis of homomorphic crypto-systems suitable for governmental electronic voting systems. From the analysis, I²R designs a new cryptographic scheme with improved properties suitable for electronic voting. A homomorphic cryptosystem allows operation to be carried on

encrypted text such as e-voting where the operation is to sum up ballots without revealing the details of the ballots.

According to experts from EADS, the outcome of this Singaporean project has been optimized for hardware implementation in cryptographic application-specific integrated circuits (ASICs) to be used in EADS' world-leading product lines.

Notes to Editor:

EADS is a global leader in aerospace, defence and related services. In 2006, EADS generated revenues of € 39.4 billion and employs a workforce of about 116,000.

EADS Singapore Research & Technology Centre is an extension of the Research Organization within the EADS Group ("EADS Innovation Works") driven by its Global Industrial Development strategy. It manages projects for the EADS business units and EADS Innovation Works while performing its activities in close cooperation with Singaporean scientific institutions.

The Agency for Science, Technology and Research, or A*STAR, is Singapore's lead agency for fostering world-class scientific research and talent for a vibrant knowledge-based Singapore.

A*STAR actively nurtures public sector research and development in Biomedical Sciences, Physical Sciences and Engineering, with a particular focus on fields essential to Singapore's manufacturing industry and new growth industries. It oversees 14 research institutes and supports extramural research with the universities, hospital research centres and other local and international partners. At the heart of this knowledge intensive work is human capital. Top local and international scientific talent drive knowledge creation at A*STAR research institutes. The Agency also sends scholars for undergraduate, graduate and post-doctoral training in the best universities, a reflection of the high priority A*STAR places on nurturing the next generation of scientific talent. (www.a-star.edu.sg)

The Institute for Infocomm Research (I²R - pronounced as i-squared-r) is a member of the Agency for Science, Technology and Research (A*STAR) family. Established in 2002, our mission is to be the globally preferred source of innovations in 'Interactive Secured Information, Content and Services Anytime Anywhere' through research by passionate people dedicated to Singapore's economic success. I²R performs R&D in information, communications and media (ICM) technologies to develop holistic solutions across the ICM value chain. Our research capabilities are in information technology and science, wireless and optical communications, and interactive digital media. We seek to be the infocomm and media value creator that keeps Singapore ahead. (www.i2r.a-star.edu.sg)

Media Contacts:

Wolfgang Reinert
Media Relations Germany, Technology Communications
Tel.: +49 (0) 89 607 27 905
Email: wolfgang.reinert@eads.com

Liong Kit Yin
Assistant Manager, Corporate Communications
Institute for Infocomm Research (I²R)
DID: (65) 6874 5232
Email: liongky@i2r.a-star.edu.sg