



Contact: Klaus-Michael Koch
E-mail: coordination@cace-project.eu
Phone: +43 4242 233 55
Website: www.cace-project.eu

PRESS RELEASE
- FOR IMMEDIATE RELEASE -

CACE TOOLS: BOOSTING SECURITY IN COMMUNICATION DEVICES!

At a glance:

CACE, a collaborative research project on Computer Aided Cryptography Engineering, recently hit the finish line. A cryptographic toolbox with security-aware high-level programming languages and compilers has been developed and published by means of open source modules. CACE tools allow automatic generation of high quality cryptographic software on different abstraction levels, ranging from high-level cryptographic protocols, over libraries for secure communication, to low-level side-channel resistant implementation of cryptographic primitives and their formal verification. The benefits are, amongst others, better quality and more robust cryptographic software at lower cost.

Main achievements:

The CACE tools set a de-facto standard for a user-friendly generation of secure and fast cryptographic software. They have been applied successfully to improve the implementation of cryptographic modules in a multitude of products, and to provide countermeasures against side-channel attacks. Security hardened codes for a bit-sliced implementation of the snow3G cipher have been generated and are now being used on mobile phones. To date, more than 180 million Nokia phones worldwide are running the improved 256 bit Elliptic Prime Curve implementation generated by CACE tools.

About the project:

CACE stands for Computer Aided Cryptography Engineering - a collaborative project, which was co-financed by the European Commission under the 7th Framework Programme. The project was running for 3 years, starting from January 2008 and closing in December 2010. The CACE project was rated excellent in its final review meeting in February 2011. The project has fully achieved its objectives and technical goals and has even exceeded expectations. A full set of public project deliverables as well as the main scientific publications can be found on the official project website: <http://www.cace-project.eu>

The consortium consisted of 12 partners from industry and academia situated in nine different countries: Technikon Forschungs- und Planungsgesellschaft mbH (AT), Ruhr-University Bochum (DE), University of Bristol (UK), Eindhoven University of Technology (NL), Universidade do Minho (PT), Bern University of Applied Sciences (CH), Aarhus University (DK), University of Haifa (IL), Sirrix Security Technologies AG (DE), Helsinki University of Technology (FI), Nokia (FI), Alexandra Institute (DK).

Learn more about the CACE project visiting: <http://www.cace-project.eu>

Contact: Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
E-mail: coordination@cace-project.eu
Phone: +43 4242 233 55, Fax: +43 4242 233 55 77

Disclaimer:

The content of this press release is owned by the CACE project consortium. This press release may contain forward-looking statements relating to advanced information and communication technologies. The CACE project consortium does not accept any responsibility or liability for any use made of the information provided in this press release. The FP7 logo in this press release is owned by the European Commission. The use of the logo reflects that CACE receives funding from the European Commission. Apart from this, the European Commission has no responsibility for the content.