

## Call for Papers SantaCrypt 2011

1 – 2 December, 2011, Prague, Czech Rep.

<http://mkb.buslab.org>

### Intro

Santa's Crypto Get-Together (SantaCrypt) started in 2001 as the first annual Czech and Slovak workshop aiming to facilitate closer cooperation of professionals working in the field of applied cryptography and related areas of security. This get-together of experts is organised in order to foster exchange of information and ideas on past, ongoing, and also future projects. We recognise the need of experts meeting their colleagues without the hassle of taking care of their (potential) customers, bosses and other distracting forces. ;-) The workshop is run in English in the first day and then Czech and Slovak the second day.

There will be five invited lectures:

- Chris Mitchell (Royal Holloway, UK): *New architectures for identity management - removing barriers to adoption.*
- Graham Steel (INRIA, France): *Attacking and Fixing PKCS#11 Security Tokens.*
- Viktor Fischer (Jean Monnet University Saint-Etienne, France): *Recent Advances in Random Numbers Generation for Cryptography.*
- Pavel Vondruška (Telefónica O2 Czech Rep.): *Ciphers used by Czechoslovak personalities.*
- Jozef Kollár (Slovak U. of Techn., Bratislava, Slovakia): *Czechoslovak ciphers of World War II.*

Detailed information, including registration guidelines, will be available in due course on workshop web pages: <http://www.buslab.cz/mkb>.

### Instructions for Authors

The program committee will accept submissions targeting cryptanalysis, cryptography, security applications of cryptography and other related areas. Proposals should be of 5-15 pages and formatted for anonymous evaluation. Word and LaTeX templates for submissions are also available from the workshop web: <http://mkb.buslab.org>. Submissions can be written in Czech, Slovak, or English.

Submissions should be mailed to [matyas AT fi.muni.cz](mailto:matyas@fi.muni.cz), and clearly marked with Subject "SantaCrypt 2011". The final deadline for the submissions is *3<sup>rd</sup> October 2011*. Submissions will be evaluated by the program committee and authors will be informed about the evaluation results by *31<sup>st</sup> October*. Camera-ready versions for the workshop proceedings have to be delivered by *14<sup>th</sup> November*.

### Important Dates

Submission deadline:	3 <sup>rd</sup> October, 2011
Acceptance/rejection notification:	31 <sup>st</sup> October, 2011
Camera-ready format:	14 <sup>th</sup> November, 2011
Workshop:	1 <sup>st</sup> – 2 <sup>nd</sup> December, 2011



### Program Committee

Dan Cvrček, Smart Architects, UK  
 Vlastimil Klíma, KNZ, CZ  
 Vashek Matyáš, Masaryk U., Brno, CZ – Chair  
 Tomáš Rosa, Raiffeisenbank & Charles U., CZ

Luděk Smolík, Siegen, Germany  
 Martin Stanek, Comenius U., Slovakia  
 Petr Švenda, Masaryk U., Brno, CZ