Mikulášská kryptobesídka

2. prosince 2002 (Pondělí)
Hotel Olšanka, Táboritská 23, Praha 3

15:00 - 16:00 Registrace
16:00 - 16:10 Zahájení workshopu

Public Key Infrastructures I

16:10 - 16:55 Geraint Price - Public Key Instrastructures: where next?
Prostor pro diskuzi k tématu

± 17:05 - 17:35 Daniel Cvrček - Vytvoření lokální klíčové infrastruktury
Prostor pro diskuzi k tématu

± 17:45 - 18:05 Jan Hobza - Profil kvalifikovaného certifikátu
Prostor pro diskuzi k tématu

Následuje série neformálních diskuzí v prostorách restaurace vyhrazených pouze pro účastníky kryptobesídky.

3. prosince 2002 (Úterý)
Hotel Olšanka, Táboritská 23, Praha 3

8:30 - 9:00 Registrace
9:00 - 9:10 Zahájení druhého dne workshopu

Nové algoritmy a postupy

9:05 - 9:50 Vincent Rijmen - Beyond the AES
Prostor pro diskuzi k tématu

± 10:00 - 10:30 Lenka Fibíková - Towards proper selection of primitives and modifications for a cryptographic scheme
Prostor pro diskuzi k tématu

do 11:00 Přestávka na kávu

Mediální partneři:

CryptoWorld

do 11:00 Přestávka na kávu

± 11:00 - 11:20 Karel Burda - The solving of equation systems in Boolean Ring
Prostor pro diskuzi k tématu

± 11:30 - 12:00 Bohuslav Rudolf - Diffusion Evaluation Matrix Applied to (Generalized) Feisteli Networks
Prostor pro diskuzi k tématu

do 13:30 Oběd

Implementace

13:30 - 14:15 Ingo Schubert - Making Security Fit
Prostor pro diskuzi k tématu

do 14:45 Přestávka na kávu

± 14:45 - 15:15 Pavel Vondruška, Jan Hobza - Bezpečnostní požadavky na ISCS v ČR a EU (ISCS - Informační systémpro certifikační služby)
Prostor pro diskuzi k tématu

± 15:22 - 17:00 Panelová diskuze „PKI včera, dnes a zítra“

Panelisté: Tonda Beneš
Dan Cvrček
Daniel Olejár
Jaroslav Pinkava
Tomáš Rosa
Jozef Vyskoč - moderátor

Závěr workshopu

Mediální partneři:

CryptoWorld