www.opentc.eu

Open Trusted Computing

avagy mitől lesz bizalomra méltó a számítástechnika?

Hornák Zoltán

OpenTC tanszéki ismertető

2007 november 28

Trusted Computing

- TCG – Trusted Computing Group által definiált követelmények a „Bizalomra méltó számítástechnikával” szemben
  - Sok munkacsoport
  - Több ezer oldalnyi dokumentáció
- TPM – Trusted Platform Module
  - HW chip
  - Biztonság-kritikus funkciók megvalósítása
    - rejtjelkulcsok biztonságos tárolása
    - digitális aláírás
    - rejtjelezett hard diszk
    - Virtualizáció
- TSS – Trusted Software Stack
  - Biztonsági funkciók megbízható implementálása

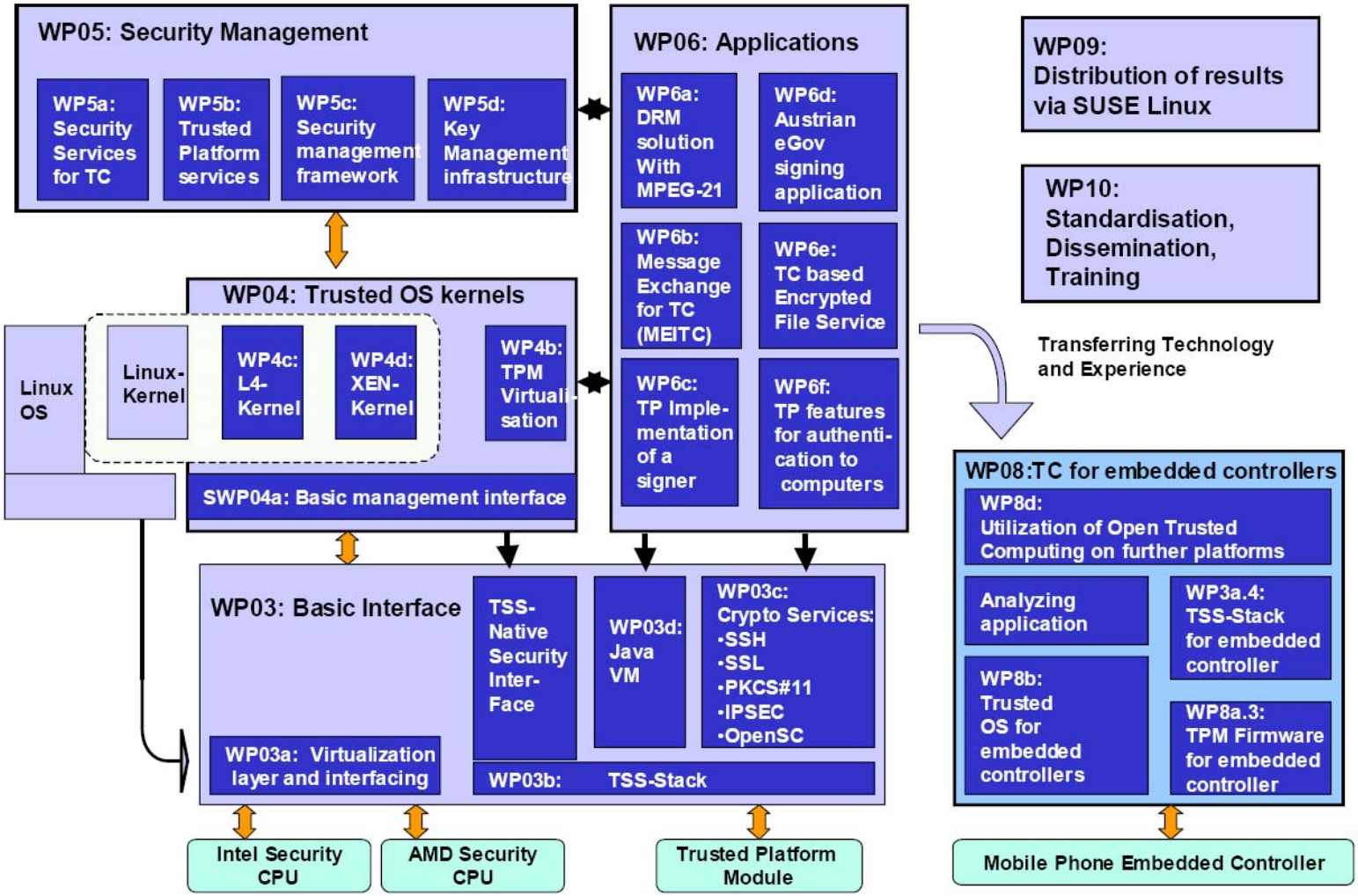
Az OpenTC project

- Célkitűzések
  - Nyílt forráskódú TCG követelményeknek megfelelő TPM támogatás
  - Lényeges biztonsági funkciók megbízható megvalósítása
    - Virtualizáció
    - Hard diszk rejtjelezés
    - Digitális aláírás
    - DRM Digital Rights Management
- Konzorciumi összetétel
  - Technikon (AT) konzorcium vezető KKV
  - IBM, HP számítógépek
  - AMD, INFINEON TPM chipek
  - SUSE (Novell) Linux támogatás
  - L4, XEN virtualizáció
  - SME és akadémiai résztvétel

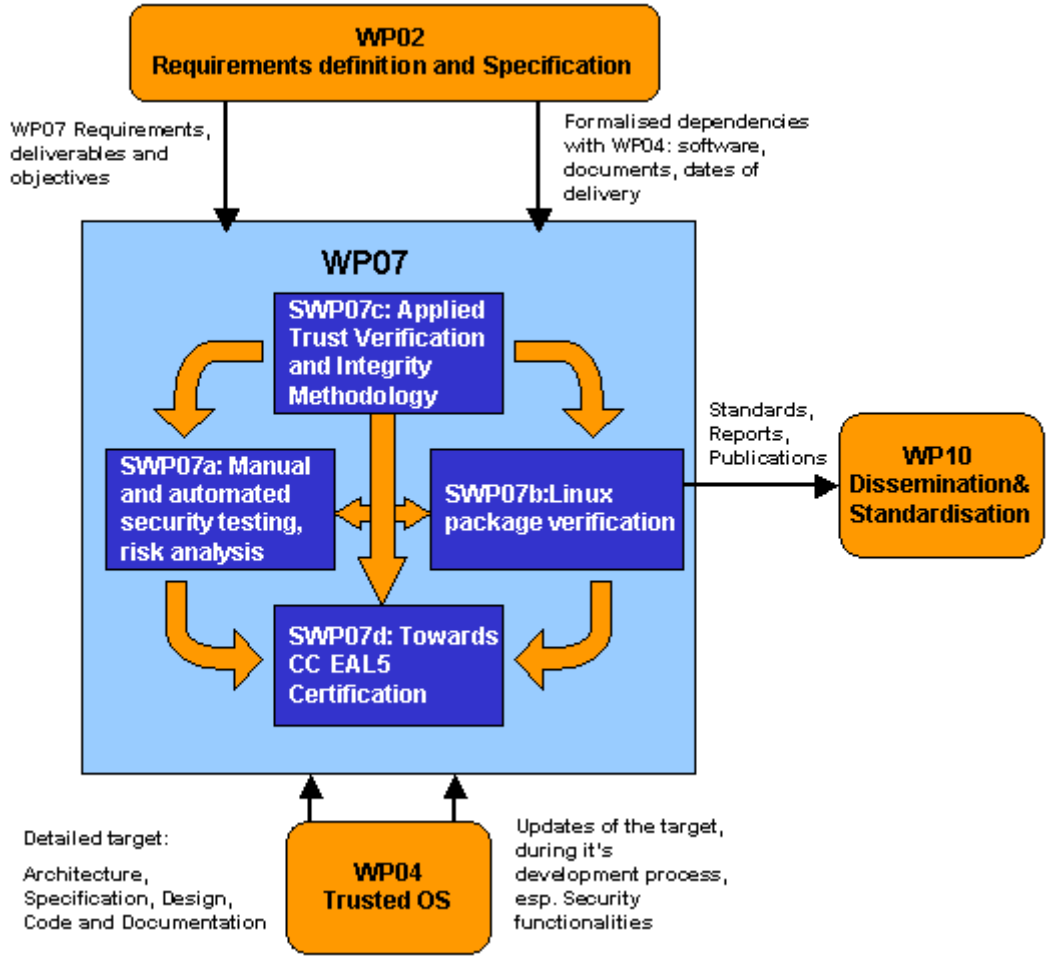
Projekt adatok

- Futamidő: 2005. november 1 – 2009. árpilis (3 és fél év)
- Résztvevők: 22 partner
  - **Ipari partnerek**: Technikon (AT), Hewlett Packard (UK), IBM Research GmbH (CH), AMD (DE), Infineon (DE), SUSE LINUX GmbH (DE), Portakal (TR)
  - **Non-profit szervezetek**: Forschungszentrum ITAS (DE), Commissariat à l'Energie Atomique (FR), ISECOM (ES)
  - **Egyetemek**: University of Technology Graz (AT), Technical University Munich (DE), Royal Holloway University of London (UK), Politecnico di Torino (IT), Budapest University of Technology and Economics (HU), Tubitak (TR), Ruhr-University Bochum (DE), Technische Universität Dresden DE, University of Cambridge UK, Technical University of Sofia (BG), Katholieke Universiteit LeuvenKlaus (BE)
- Költségvetés:
  - 17 MEur összköltség
  - 12 MEur támogatás

Projekt felépítése



WP7 – Validáció és verifikáció (V&V)



Célkitűzés:

A projekt keretén belül elkészült szoftverek forráskód és tesztelés alapú verifikációja és validációja

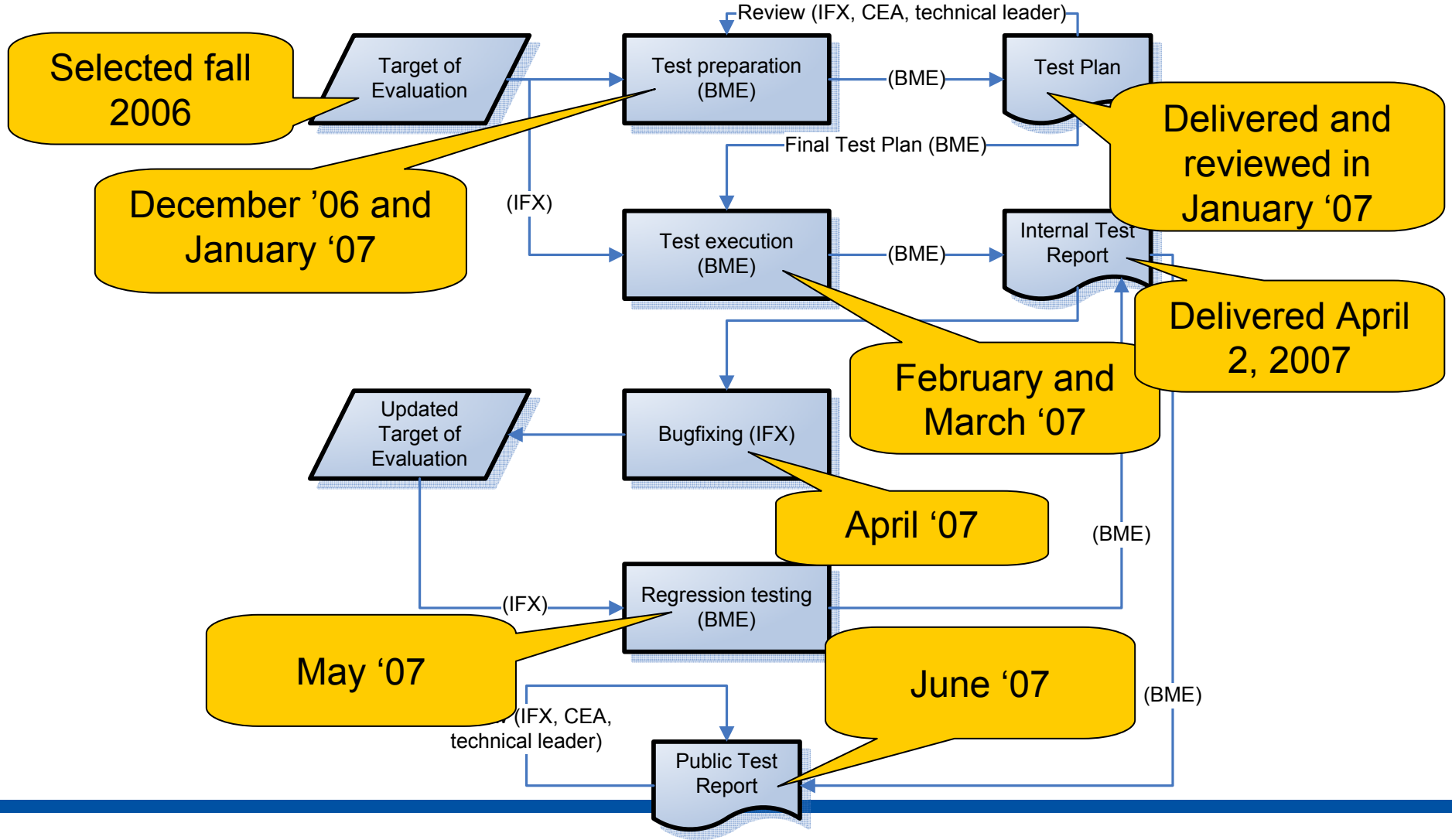
BME szerepe:

SWP7a: manuális és automatizált biztonsági tesztelés, kockázatelemzés

Biztonsági tesztelés eddigi eredményei

- SWP7a biztonsági tesztelési feladatai
  - Az OpenTC projekt keretében elkészült modulok folyamatos manuális és automatizált biztonsági tesztelése
  - A tesztelés céljait a WP7 vezetése a fejlesztőkkel és a technikai vezetőkkel közösen határozza meg
  - Az első tesztelési célpont az Infineon TSS-e volt
- Automatizált tesztelés a Flinder segítségével (www.flinder.hu)
  - Biztonsági és robosztusság tesztelés fuzzing módszerrel
  - black-box és white-box tesztelés
  - Linux támogatás kifejlesztése

Tesztelés, javítás folyamata

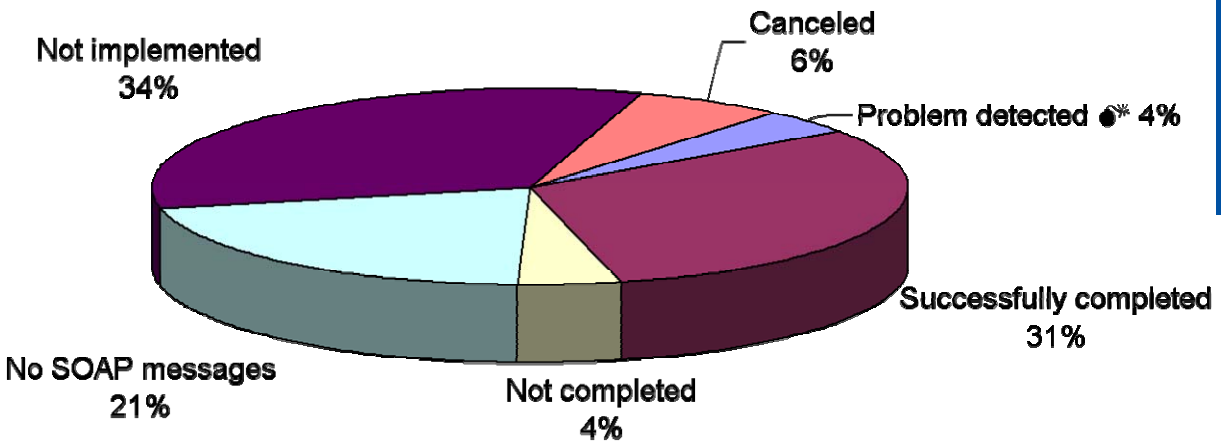


Teszt eredmények

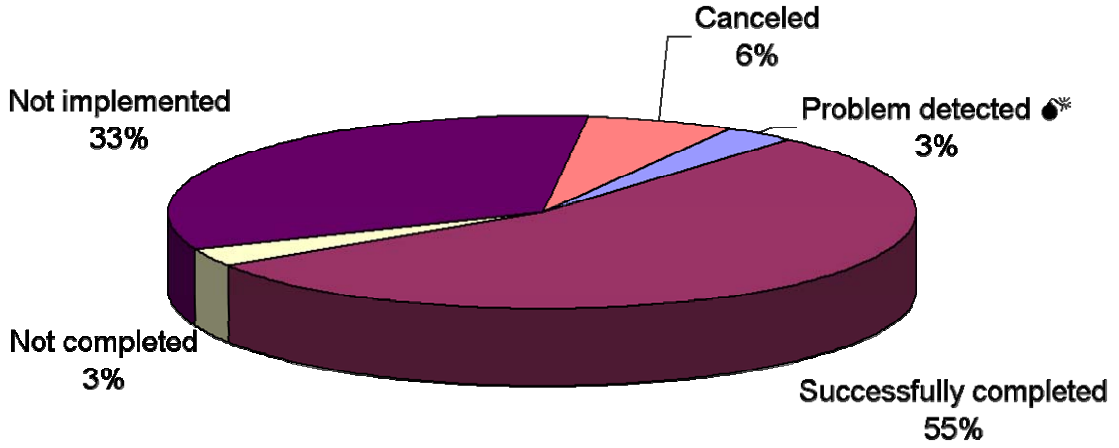
- 135.237 végrehajtott teszt eset
  - 38.106 black-box mód (33 funkciót vizsgálva)
    - 249 teszt eset megbukott (0.7%), 4 érintett funkció (12%)
    - 37.857 sikeres teszt eredmény
  - 97.131 white-box mód (54 funkciót vizsgálva)
    - 154 teszt eset megbukott (0.2%), 3 érintett funkció (6%)
    - 96.977 sikeres teszt eredmény
- 8 kihasználható gyengeség 7 függvényben
  - 6 potenciális integer kezelési hiba
    - aritmetikai túlcsurdulás, rossz cast-olás
  - 2 Puffer túlcsordulás (buffer overflow)
    - igazoltan kihasználható `memcpy()` hiba!

Teszt eredmények elemzése

Results of black-box testing

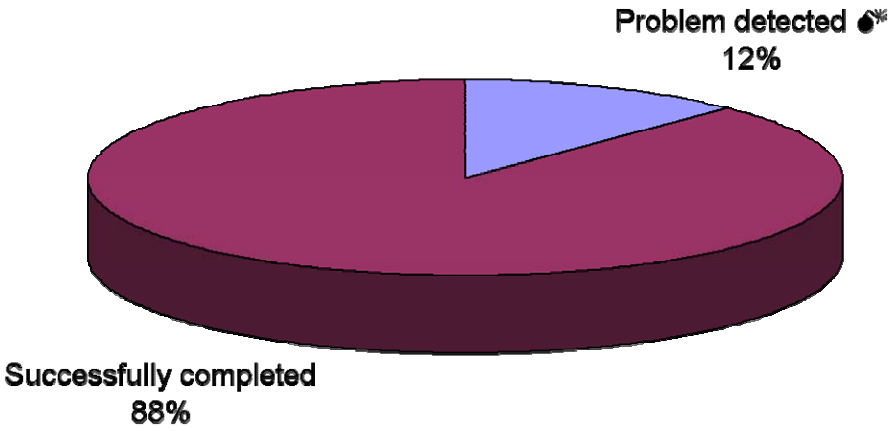


Results of white-box testing

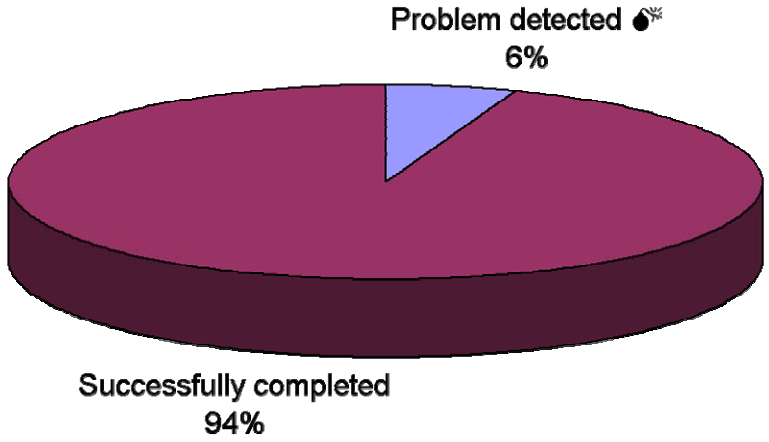


Sikeresen lefuttatott teszt esetek

Results of black-box testing



Results of white-box testing



Statisztikák

Indicates the **efficiency of the plan**

Demonstrates **ratio of weak implementations** among the API functions

Shows **efficiency of Flinder**

		Number of TSS functions				Ratio of tested functions				Number of executed tests			
		Black-box		White-box		Black-box		White-box		Black-box		White-box	
Problem detected		4	4.3%	3	3.2%	4	12.1%	3	5.6%	249	0.7%	154	0.2%
Successfully passed		29	30.9%	51	54.3%	29	87.9%	51	94.4%	37857	99.3%	96977	99.8%
Not tested	Not completed	4	4.3%	3	3.2%								
	No SOAP messages	20	21.3%	n/a	n/a								
	Not implemented	31	33.0%	31	33.0%								
	Canceled	6	6.4%	6	6.4%								
Total		94		94		33		54		38106		97131	

Kérdések?

Hornák Zoltán

Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék
hornak@mit.bme.hu

The Open-TC project is co-financed by the EC.

If you need further information, please visit our website www.opentc.eu or contact the coordinator:

Technikon Forschungs- und Planungsgesellschaft mbH
Richard-Wagner-Strasse 7, 9500 Villach, AUSTRIA
Tel. +43 4242 23355 – 0
Fax. +43 4242 23355 – 77
Email coordination@opentc.eu