

Biztonság és adatvédelem telekommunikációs és egészségügyi alkalmazásokban

Nyitórendezvény
2017. október 27.



M Ű E G Y E T E M 1 7 8 2



PÁZMÁNY PÉTER
KATOLIKUS EGYETEM

3in



EFOP-3.6.2-16-2017-00013

SZÉCHENYI 2020



MAGYARORSZÁG
KORMÁNYA

Európai Unió
Európai Szociális
Alap



BEFEKTETÉS A JÖVŐBE

A csapat

- ELTECRYPT kutatócsoport
 - IK, TTK, EIT
- 5 senior kutató
- 2 posztdoktor
- 4 doktorandusz
- hallgatók

3in

EFOP-3.6.2-16-2017-00013

ELTE - BME - PPKE

SZÉCHENYI 2020



Európai Unió
Európai Szociális
Alap



BEFEKTETÉS A JÖVŐBE

Korábbi EIT K+F projektek

Engineering Privacy and Security in Crowdsourcing along all Components

- 2014-2016, S&P action line
- TU Berlin
- Biztonságos Crwodsourcing módszerek és alkalmazások üzleti környezetre
- Új üzleti modellek
- Start-Up
- ELTE feladat
 - Létező alkalmazások biztonsági elemzése
 - Gamifikáció, lokáció

3in

EFOP-3.6.2-16-2017-00013

ELTE - BME - PPKE

SZÉCHENYI 2020



Európai Unió
Európai Szociális
Alap



BEFEKTETÉS A JÖVŐBE

Korábbi EIT K+F projektek

FIDES: Federated Identity Management System

- 2014-2015, S&P action line
- Poste Italiane
- IDM keretrendszer
 - Követelmények
 - Implementáció
 - Alkalmazások
- ELTE feladat
 - Tároló médiumok követelményei
 - Szavazó alkalmazás

3in

EFOP-3.6.2-16-2017-00013

ELTE - BME - PPKE

SZÉCHENYI 2020



Európai Unió
Európai Szociális
Alap



BEFEKTETÉS A JÖVŐBE

Jövőbeli EIT K+F projekt

OFION – Orchestration of financial services on-demand

- 2017-2018, Digital Finance action line
- ATOS
- Felhő-alapú üzleti szolgáltatások összehangolása
- ELTE feladat:
 - Blockchain PoC

3in

EFOP-3.6.2-16-2017-00013

ELTE - BME - PPKE

SZÉCHENYI 2020



Európai Unió
Európai Szociális
Alap



BEFEKTETÉS A JÖVŐBE

Kutatási témák

- Kis energiaigényű titkosítási protokollok kialakítása
- Hatékony differenciális adatvédelem és homomorf titkosítás speciális célokra

3in

EFOP-3.6.2-16-2017-00013

ELTE - BME - PPKE

SZÉCHENYI 2020



Európai Unió
Európai Szociális
Alap



BEFEKTETÉS A JÖVŐBE

Kis energiaigényű titkosítási protokollok

- Szenzorok által gyűjtött és továbbított adatok védelme
- Minimalista kriptográfia
 - Számítási, kommunikációs, tárolási bonyolultság
- Elosztott protokollok
- Titokmegosztások

3in

EFOP-3.6.2-16-2017-00013

ELTE - BME - PPKE

SZÉCHENYI 2020



Európai Unió
Európai Szociális
Alap



BEFEKTETÉS A JÖVŐBE

Differenciális adatvédelem és homomorf titkosítás

- Biztonságos számítások felhőben tárolt adatokon
- Általános megoldások nem hatékonyak
- Konkrét alkalmazásokhoz illeszkedő megoldások
- Egyszerű műveletek

3in

EFOP-3.6.2-16-2017-00013

ELTE - BME - PPKE

SZÉCHENYI 2020



Európai Unió
Európai Szociális
Alap



BEFEKTETÉS A JÖVŐBE