ANEXA 2

Universitatea "Alexandru Ioan Cuza" din Iaşi[1]

FIŞA DE EVIDENŢĂ Nr. 168 - 1/ 2016

a rezultatelor activităţilor de cercetare-dezvoltare

TABEL NR. 1[2]

DENUMIREA PROIECTULUI	Autentificare mutuala si managementul cheilor folosind criptografie bazata pe identitate,fara key-escrow si functii de imperechere			**CATEGORIA DE PROIECT** . PNCDI II- Subprogram Proiecte colaborative de cercetare aplicativa	
CONTRACT DE FINANŢARE	**NR** 17. **DATA** 01/07/2014	**DURATA CONTRACT**	30... **LUNI**	**ACRONIM PROGRAM**	Parteneriate
VALOAREA PROIECTULUI (INCLUDE ŞI ALTE SURSE)	. 1437491. **LEI**	**VALOAREA CONTRACTULUI DE FINANŢARE (BUGET DE STAT)**		1249991... **LEI**	
REZULTATELE CERCETĂRII APARŢIN	**1** .Universitatea "Alexandru Ioan Cuza" din Iasi....[3] **2** . Institutul pentru Tehnologii Avansate 3. INTERNIO SYSTEMS SRL		**CONFORM ART** ..... **DIN CONTRACTUL NR** .17/2014..		

1) DENUMIRE REZULTAT[4]	Publicaţii ştiinţifice			
2) CATEGORIA REZULTATULUI (conform art. 74, O.G. 57/2002)	**Rezultat final**	**Rezultate[5] intermediare**	**CARACTERISTICI ALE REZULTATULUI FINAL**	
2.1 documentaţii, studii, lucrări	x	☐	1. S. Iftene, F.L. T¸ iplea: Authentication and Key Management in VoIP and SONs, Research Report, Project PN-II-PT-PCCA-2013-4-1651, "Alexandru Ioan Cuza" of Iasi, 2014 2. F.L. T¸ iplea, S. Iftene, A.M. Nica: Identity-based Cryptography, Research Report, Project PN-II-PT-PCCA-2013-4-1651, "Alexandru Ioan Cuza" of Iasi, 2014 3. G.D. N˘astase F.L. T¸ iplea: On a Lightweight Authentication Protocol for RFID Systems, 8th International Conference on Security for InformationTechnology and Communications, SECITC 2015, June 11-12, 2015, Lecture Notes on Computer Science 9522. 4. F.L. Tiplea, E. Simion: New Results on Identity-based Encryption from Quadratic Residuosity, 8th International Conference on Security for Information Technology and Communications, SECITC 2015, June 11-12, 2015, Lecture Notes on Computer Science 9522. 5. N. Ros¸ia, V. Cervicescu,M. Togan: EfficientMontgomeryMultiplication on GPUs, 8th International Conference on Security for Information Technology and Communications, SECITC 2015, June 11-12, 2015, Lecture Notes on Computer Science 9522.	 7
2.2 planuri, scheme	☐	☐		
2.3 tehnologii	☐	☐		
2.4 procedee, metode	☐	☐		
2.5 produse informatice	☐	☐		
2.6 reţete, fromule	☐	☐		
2.7 obiecte fizice / produse	☐	☐		
2.8 brevet invenţie / altele asemenea	☐	☐		
3) STADIUL DE DEZVOLTARE	3.1 soluţie/ model conceptual	☐		
	3.2 model experimental/ funcţional	☐		
	3.3 prototip	☐		
	3.4 instalaţie pilot sau	☐		

[1] denumirea persoanei juridice executante (persoană juridică executantă este considerată persoana juridică care a obţinut rezultatele cercetării, în mod nemijlocit, conform art. 74 alin. (3) din O.G. nr. 57/2002)

[2] se completează o singură dată, la 30 de zile de la data aprobării raportului de activitate al proiectului de cercetare-dezvoltare

[3] se completează denumirea partenerilor la proiectul de cercetare-dezvoltare care au contribuit la obţinerea rezultatului

[4] se trece denumirea rezultatului cercetării (nu se trece denumirea proiectului)

[5] se trec rezultatele cercetării din etapele intermediare ale proiectului de cercetare-dezvoltare care pot fi utilizate / valorificate independent de includerea în rezultatul final

[7] se inserează poza rezultatului / produsului final

	echivalent		6. F.L. T¸ iplea: Sharing Secrets on Boolean Circuits: Application to Key-policy Attribute-based Encryption, invited talk, Romanian Cryptology Days, Sept 21-23, 2015, Bucharest (Romania). 7. Andrei Marghescu, Paul Svasta, and Emil Simion. Randomness extraction techniques for jittery oscillators. In 2015 38th International Spring Seminar on Electronics Technology (ISSE), pages 161–166. IEEE, 2015. 8. AndreiMarghescu, Paul Svasta, and Emil Simion. Optimising ring oscillatorbased true random number generators concept on fpga. In Electronics Technology (ISSE), 2016 39th International Spring Seminar on, pages 149–153. IEEE, 2016. 9. Andrei Marghescu and Paul Svasta. Pushing the optimization limits of ring oscillator-based true random number generators. In International Conference for Information Technology and Communications, pages 209–224. Springer, 2016. 10. Emil Simion. The relevance of statistical tests in cryptography. IEEE Security & Privacy, 13(1):66–70, 2015. 11. Ferucio Laurentiu T¸ iplea, Sorin Iftene, George Teseleanu, and Anca Maria Nica. Security of identity-based encryption from quadratic residuosity. In International Conference for Information Technology and Communications, pages 63–77. Springer, 2016..... [6]
	3.5 altele	☐	
4) DOMENIUL DE CERCETARE	4.1 tehnologiile societăţii informaţionale	x	
	4.2 energie	☐	
	4.3 mediu	☐	
	4.4 sănătate	☐	
	4.5 agricultură, securitatea şi siguranţa alimentară	☐	
	4.6 biotehnologii	☐	
	4.7 materiale, procese şi produse inovative	☐	
	4.8 spaţiu şi securitate	☐	
	4.9 cercetări socio-economice şi umaniste	☐	
5) DOMENII DE APLICABILITATE[8]	72 ; ☐☐ ; ☐☐		
6) CARACTERUL INOVATIV	6.1 produs nou	☐	Autentificarea Mutuală și KeyManagement sunt componente esențiale ale tuturor tehnicilor de securitate încorporate în tehnologiile de comunicare de astăzi, cum ar fi IPsec, SSL și TLS, Voice over IP (VoIP) și rețelele de auto-organizare (SONS). Tehnicile existente se bazează în principal pe infrastructuri cu cheie publică (PKI) care au multe deficiențe practice evidențiate de mulți cercetători și practicieni, ceea ce le face impracticabile pentru sistemele mari sau pentru sistemele foarte dinamice cu putere computațională limitată (cum ar fi mobile ad hoc sau sensor networks)... [9]
	6.2 produs modernizat	☐	
	6.3 tehnologie nouă	☐	
	6.4 tehnologie modernizată	☐	
	6.5 serviciu nou	☐	
	6.6 serviciu modernizat	☐	
	6.7 altele	x	

INFORMAŢII PRIVIND PROPRIETATEA INTELECTUALĂ		
documentaţie tehnico-economică	☐	
cerere înregistrare brevet de invenţie	☐	nr. ..... data .....
brevet de invenţie înregistrate (naţional, european, internaţional)	☐	nr. ..... data .....
cerere înregistrare modele şi desene industriale protejate	☐	nr. ..... data .....
modele şi desene industriale protejate înregistrate (naţional, european, internaţional)	☐	nr. ..... data .....
cerere înregistrare marcă înregistrată	☐	nr. ..... data .....
mărci înregistrate (naţional, european, internaţional)	☐	nr. ..... data .....
cerere înregistrare copyright	☐	nr. ..... data .....
înregistrare copyright (naţional, european, internaţional)	☐	nr. ..... data .....
cerere înregistrare: reţele, indicaţii geografice, specii vegetale şi animale, etc.	☐	nr. ..... data .....
înregistrare: reţele, indicaţii geografice, specii vegetale şi animale, etc. (naţional,	☐	nr. ..... data .....

[6] se prezintă structura, datele tehnice, parametrii de funcţionare specifici rezultatului final
[8] conform CAEN 2008, 2 cifre
[9] justificare (se explică, în maximum 100 caractere, în ce constă noutatea)

european, international)		

TABEL NR. 2[10]

7)[11] VALORIFICAREA REZULTATELOR CERCETĂRII

8) DENUMIREA REZULTATULUI DE CERCETARE .....[12]

NR CRT.	VALOAREA DE LA CARE ÎNCEPE NEGOCIEREA	PROCES VERBAL[13] NR./DATA	MOD DE VALORIFICARE[14]	ACTUL[15] PRIN CARE S-A REALIZAT VALORIFICAREA	VALOAREA NEGOCIATĂ[16]	BENEFICIAR[17]	IMPACT[18]	PERSOANE AUTORIZATE[19]
0	1	2	3	5	6	7	8	9
1			Publicare literatura stiintifica			Universitatea "Alexandru Ioan Cuza" din Iasi....[20] Institutul pentru Tehnologii Avansate INTERNIO SYSTEMS SRL		Tiplea Ferucio Laurentiu
2								
3								

Director de proiect,
Tiplea Ferucio Laurentiu

---

[10] se completează în termen de 10 zile de la data finalizării activităţilor de valorificare a rezultatului cercetării
[11] se actualizează pentru fiecare acţiune de valorificare a rezultatului cercetării
[12] se va trece denumirea rezultatului final sau, după caz, a rezultatului(lor) intermediar(e)
[13] se vor trece numărul şi data la care a fost încheiat procesul verbal al comisiei constituite la nivelul persoanei juridice executante care a stabilit valoarea de la care începe negocierea şi se precizează codul procedurii specifice, aprobată la nivelul organului cu atribuţii de conducere (ex. consiliul de administraţie), în baza căreia se realizează valorificarea rezultatelor obţinute în urma activităţilor de cercetare-dezvoltare, cu respectarea reglementărilor legale în vigoare;
[14] vânzare produs/tehnologie; furnizare servicii; închiriere, concesionare, preluare în producţia proprie, transmitere cu titlu gratuit; transfer drepturi de proprietate intelectuală;
[15] se va trece nr. şi data semnării actului (ex. contract) prin care s-a realizat valorificarea rezultatului cercetării;
[16] valoarea rezultatelor cercetării este stabilită la preţul negociat între părţi.
[17] se completează denumirea beneficiarului care preia rezultatul cercetării (date de contact operator economic, adresă, oraş, judeţ, telefon, fax, e-mail, website)
[18] se vor completa efectele (economice, sociale, de mediu) obţinute la beneficiar asociate aplicării rezultatelor cercetării, anual, pentru o perioadă de 5 ani
[19] numele şi semnătura persoanei autorizate să completeze fişa de evidenţă şi al persoanei din cadrul compartimentului financiar-contabil responsabil cu verificarea datelor.
[20] se completează denumirea partenerilor la proiectul de cercetare-dezvoltare care au contribuit la obţinerea rezultatului