Oznaka poročila: ARRS-RPROJ-ZP-2010-1/57

ZAKLJUČNO POROČILO
O REZULTATIH RAZISKOVALNEGA PROJEKTA

A. PODATKI O RAZISKOVALNEM PROJEKTU

1. Osnovni podatki o raziskovalnem projektu

Šifra projekta	J2-9649
Naslov projekta	Lahke kriptografske storitve za upravljanje varnosti, zasebnosti in zaupanja - LaKS
Vodja projekta	12765 Roman Novak
Tip projekta	J Temeljni projekt
Obseg raziskovalnih ur	3.150
Cenovni razred	C
Trajanje projekta	01.2007 - 12.2009
Nosilna raziskovalna organizacija	106 Institut "Jožef Stefan"
Raziskovalne organizacije - soizvajalke	1538 Univerza v Ljubljani, Fakulteta za elektrotehniko 1539 Univerza v Ljubljani, Fakulteta za računalništvo in informatiko 1669 Univerza na Primorskem, Primorski inštitut za naravoslovne in tehnične vede Koper
Družbeno-ekonomski cilj	13. Splošni napredek znanja - RiR financiran iz drugih virov (ne iz splošnih univerzitetnih fondov - SUF)

2. Sofinancerji[1]

1.	Naziv	
	Naslov	
2.	Naziv	
	Naslov	
3.	Naziv	
	Naslov	

B. REZULTATI IN DOSEŽKI RAZISKOVALNEGA PROJEKTA

3. Poročilo o realizaciji programa raziskovalnega projekta[2]

Skladno z dokumentacijo, na osnovi katere je bil odobren projekt, so bili generalni cilji predlaganega projekta sledeči:

1. Storitve za varnost, zasebnost in zaupanje morajo biti optimizirane, bolje rečeno minimizirane, da je moč zagotoviti želeno varnostno funkcionalnost v okoljih z

omejenimi resursi (konkretno okolja RFID, pa tudi senzorska omrežja). Zatorej je potrebno razviti nove družine storitev ali pa minimizirati obstoječe. V ta namen potrebujemo ustrezne metodologije, da bi dobili želene lahke storitve.
2. Varnost lahko tretiramo v veliki meri s tehnološkega vidika, za zasebnost in zaupanje pa je potreben dodaten poudarek. Razlog je ta, da je uporabnikova percepcija in njegovo obnašanje tu v ospredju, kar zahteva prilagojene metodologije in tehnološke rešitve. Te imajo domicil (tudi) v domeni modeliranja uporabnikov in njihove podpore.
3. Razvoj formalizma, ki bi omogočal kvantitativno vrednotenje tega, kdaj je nek protokol (varnostna storitev) lahka in kdaj ne.

V začetku projekta (v letu 2007) smo se osredotočili predvsem na proučevanje obstoječih kriptografskih protokolov, kjer smo ugotavljali njihovo primernost za uporabo v okoljih z omejenimi računskimi, sistemskimi in komunikacijskimi viri. Zato smo se osredotočili na simetrične bločne kriptosisteme (ang. symmetric block ciphers) in na močne enosmerne zgoščevalne funkcije (ang. strong one-way hash functions). Od obstoječih simetričnih kriptografskih algoritmov smo podrobneje analizirali DES, 3DES, IDEA, AES, pri močnih enosmernih zgoščevalnih funkcijah pa MD2, SHA-1, MD4 in MD5. Pri analizi teh postopkov smo se osredotočili predvsem na računsko zahtevnost posameznih operacij v postopkih, na sistemske zahteve postopkov pri shranjevanju podatkov in vmesnih rezultatov operacij ter na porabo energije (moči) pri njihovi izvedbi. Na podlagi te analize smo identificirali, kateri od obstoječih postopkov oziroma katere skupine operacij so najbolj primerne za razvoj lahkih kriptografskih rešitev in te smo uporabili v nadaljevanju. Prvenstveno so za naše namene kot primerne od simetričnih postopkov identificirali DESL (Lightweight DES), ki smo ga uporabili za učinkovito generiranje naključnih vrednosti, nakar pa smo (kar je morda nenavadno) uporabili princip »one-time pad« tekočih šifer in dobili t.i. nedeterministične protokole za zagotavljanje overjanja in zasebnosti. Nedeterminizem v tem primeru pomeni, da je odziv značke RFID z določenega intervala in čitalec mora prečesati ves interval možnih vrednosti, da bi ugotovil ujemanje (je pa ta interval napram vsem možnim vrednostim tako majhen, da je verjetnost goljufije poljubno majhna, pač od velikosti intervala in npr. gradacije urinega koraka). Sama optimizacija obstoječih varnostnih storitev se namreč ni izkazala za smiselno, ker so zadeve na tem področju že zelo nizkonivojsko optimizirane, tako da smo z našim izvirnim pristopom dosegli dodatni prednost v smislu nezahtevnosti glede računskih virov. Do objave naših rezultatov nismo vedeli, da je sploh kdo že uporabil nam soroden princip, naknadno pa smo ugotovili, da je približno sočasno z nami soroden princip uporabila tudi druga skupina raziskovalcev (to je princip nedeterminističnega kripto-protokola). Ta princip smo nato uporabili za naš pristop in skupaj z gostujočim finskim raziskovalcem razvili družino lahkih nedeterminističnih protokolov za zagotavljanje overjanja in zasebnosti, ki jo je moč implementirati v obstoječih sistemih RFID. Ta rešitev je bila objavljena v zn. monografiji pri ugledni založbi CRC Press / Auerbach, poleg tega pa smo imeli s tega področja tudi prispevek na kakovostni konferenci, ki jo organizira NATO. In končno, za to rešitev smo dobili podeljen slovenski patent.

V zvezi z drugo alinejo, ki se tiče obvladovanja zaupanja pa smo razvili generičen formalizem za računsko podporo obvladovanja zaupanja. Ta se imenuje kvalitativna algebra in se je v znanstveni in s področja kvalitativne algebre smo tako objavili članek leta 2008 v reviji SCI, imeli pa smo tudi vabljeno predavanje na konferenci AIC 08. V letu 2009 pa smo objavili še en članek, ki pa se je nanašal na praktično implementacijo rešitve za podporo obvladovanja zaupanja, ki se imenuje trustGuard. S to rešitvijo smo vzbudili tudi precej zanimanja v okviru projekta COST Agreement Technologies in pa evropskega projekta SEMPOC, s katerim smo začeli v letu 2009 in ki se ukvarja z obvladovanjem varnosti kritičnih infrastruktur. Kvalitativna algebra se je izkazala za izjemno zanimiv pristop, ki ima širše polje uporabnosti, kot je bilo inicialno načrtovano – interes zanjo se kaže tudi v krogih, ki se ukvarjajo z managementom. Predstavlja namreč komplement obstoječim pristopom kot so teorija iger in Dampster-Shaferjeva teorija evidence.

V zvezi s tretjo alinejo - razvili smo tudi formalno metodologijo, ki omogoča kvantitativno vrednotenje lahkih protokolov in je koncipirana predvsem na tisti segment komunikacij, ki se trenutno najbolj razvija – senzorska in RFID omrežja (metodologija je objavljena v SCI reviji). Vendar pa je to delo pripeljalo do še pomembnejših rezultatov, ki so podani v nadaljevanju poročila.

Končno velja omeniti še problem prototipne realizacije – to je prototipno izvedbo lahkih protokolov za sisteme RFID v okoljih FPGA. Ta cilj je še v postopku realizacije in bo realiziran tekom tega leta, saj na njem dela magistrski študent Iztok Starc, ki bo magistriral v naslednjih

mesecih.

4. Ocena stopnje realizacije zastavljenih raziskovalnih ciljev[3]

Stopnja realizacije zastavljenih ciljev je na nivoju inicialnih ciljev 100% (s tem da bo preostanek realiziran še tekom tega leta, to so prototipne implementacije v okoljih RFID, ki so predmet magistrskega dela Iztoka Starca). Smo pa v določenih segmentih bistveno presegli inicialne načrte in naša lastna pričakovanja. Delo na projektu je pripeljalo do obetavnih raziskav na področju kvantitativnega obvladovanja tveganj v inf. sistemih, kjer smo uspeli rezultate celo objaviti v SCI reviji – Computer Journal, Oxford University Press. Skratka, SCI objav je več, kot smo načrtovali.

5. Utemeljitev morebitnih sprememb programa raziskovalnega projekta[4]

Projekt ni doživel nobenih sprememb – raziskave so se odvijale po predvidenem načrtu.

6. Najpomembnejši znanstveni rezultati projektne skupine[5]

	Znanstveni rezultat		
1.	Naslov	*SLO*	D. Trček, D. Kovač, A formal apparatus for modeling trust in computing environments
		ANG	D. Trček, D. Kovač, A formal apparatus for modeling trust in computing environments
	Opis	*SLO*	Članek podaja osnove novo razvitega formalizma, to je kvalitativne algebre za modeliranje uporabnikov pri obvladovanju zaupanja.
		ANG	The article presents a new formalism called qualitative algebra that is intended for user modelling to support computerized trust management.
	Objavljeno v		Mathematical and Computer Modelling, Elsevier, 2008
	Tipologija		1.01 Izvirni znanstveni članek
	COBISS.SI-ID		6557012
2.	Naslov	*SLO*	D. Trček,Assuring security in disadvantaged networks based on RFID systems
		ANG	D. Trček,Assuring security in disadvantaged networks based on RFID systems
	Opis	*SLO*	V prispevku je podana predstavitev novo razvitih lahkih protokolov za zagotavljanje varnosti in zasebnosti, poleg tega pa so izpostavljeni problemi ustreznih taksonomij za sistematično obvladovanje področja.
		ANG	This paper presents new family of lightweight protocols for security & privacy in RFID environments. The problem of appropriate taxonomies is discussed as well, because such taxonomies would enable systematic approach to finding solutions.
	Objavljeno v		NATO Information assurance for emerging and future military systems, Ljubljana, 2008
	Tipologija		1.08 Objavljeni znanstveni prispevek na konferenci
	COBISS.SI-ID		6778708
3.	Naslov	*SLO*	Kovač D., Trček D., Qualitative trust modeling in SOA
		ANG	Kovač D., Trček D., Qualitative trust modeling in SOA
	Opis	*SLO*	V prispevku je podan model in zasnova rešitve za podporo obvladovanja zaupanja v okoljih SOA.
		ANG	This paper presents a model and a technical solution for support of trust management in SOA environments.
	Objavljeno v		Journal of Sys. Architectures, Vol. 31, No. 2, pp. 255-263, Springer, 2009
	Tipologija		1.01 Izvirni znanstveni članek
	COBISS.SI-ID		6903892
4.	Naslov	*SLO*	Trček D., Security metrics foundations for computer security

		ANG	Trček D., Security metrics foundations for computer security
	Opis	*SLO*	V prispevku je podana metodologija za kvantitativno vrednotenje tega, kdaj lahko nek protokol ovrednotimo kot lahek in kdaj ne.
		ANG	This paper presents a methodology, which enables quantification of term "lightweight", i.e. it enables to judge which protocol is lightweight and which not.
	Objavljeno v		Computer Journal, Oxford University Press, pp. 1-7, doi: 10.1093/comjnl/bxn094
	Tipologija		1.01 Izvirni znanstveni članek
	COBISS.SI-ID		1024172628
5.	Naslov	*SLO*	Trček D., System dynamics based risk management for distributed inf. systems
		ANG	Trček D., System dynamics based risk management for distributed inf. systems
	Opis	*SLO*	V prispevku je podana nova metodologija, ki omogoča kvantitativno vrednotenje tveganj v informacijskih sistemih - članek je dobil nagrado »Best paper award« na konferenci IARIA ICONS 09.
		ANG	This paper presents a new methodology for quantitative risk management in information systems – it has been awarded with "The best paper award" at IARIA ICONS 09 conference.
	Objavljeno v		Proc. of ICONS 2009, str. 74-79, Gosier, IEEE, 2009
	Tipologija		1.06 Objavljeni znanstveni prispevek na konferenci (vabljeno predavanje)
	COBISS.SI-ID		6960980

7. Najpomembnejši družbeno-ekonomsko relevantni rezultati projektne skupine[6]

	Družbeno-ekonomsko relevantni rezultat		
1.	Naslov	*SLO*	Trček D., Security and privacy in RFID based wireless networks
		ANG	Trček D., Security and privacy in RFID based wireless networks
	Opis	*SLO*	To poglavje v znanstveni monografiji obravnava področje zagotavljanja varnosti in zasebnosti v okoljih RFID, kjer je glavna težava v pomanjkanju računskih virov za zagotavljanje varnosti in zasebnosti. Torej morajo novo razvite rešitve zagotoviti ustrezno stopnjo varnosti in zasebnosti na način, kjer je moč uporabiti kvečjemu dva do tri tisoč logičnih vrat.
		ANG	This chapter in scientific monograph covers the problem area of provision of security and privacy in RFID systems – the main problem is that these systems lack resources. Therefore new solutions have to be developed that can provide sufficient level of protection by using at most two to three thousand logical gates.
	Šifra		D.11 Drugo
	Objavljeno v		Handbook of research on wireless security, Hershey / New York / London, IGI Global, 2008
	Tipologija		1.16 Samostojni znanstveni sestavek ali poglavje v monografski publikaciji
	COBISS.SI-ID		6477396
2.	Naslov	*SLO*	Trček D., Managing trust in services oriented architectures
		ANG	Trček D., Managing trust in services oriented architectures
	Opis	*SLO*	Vsebina tega uvodnega vabljenega predavanja na mednarodni znanstveni konferenci je pokrivala problematiko računsko podprtega obvladovanja zaupanja s poudarkom na izvajanju v storitveno usmerjenih arhitekturah. Predstavljeni so bili glavni metodološki pristopi vključno s kvalitativno algebro.
		ANG	The content of this invited presentation at an international conference was on trust management in computerized environments with emphasis on services oriented architectures. Main current methodologies and approaches were presented together with qualitative algebra.
	Šifra		B.04 Vabljeno predavanje
			Proc. of the AIC'08, pp. 23-28, Rodos, 2008

	Objavljeno v		
	Tipologija		1.06 Objavljeni znanstveni prispevek na konferenci (vabljeno predavanje)
	COBISS.SI-ID		6604884
3.	Naslov	*SLO*	Trček D., Japinnen P., Metoda za omogočanje overjanja in zaupnosti v okoljih RFID
		ANG	Trček D., Japinnen P., A method for provision of authentication and privacy in RFID systems
	Opis	*SLO*	Ta patentna prijava podaja novo tehnološko rešitev (varnostno storitev), ki ob minimalnih zahtevah po računskih virih zagotavlja overjanje in zasebnost. Tržni potencial patenta je bil preverjen na Finskem, vendar interesa v tamkajšnji industriji ni bilo.
		ANG	This patent covers a new technical solution (security service), which provides authentication and assures privacy when deploying devices with low computational capabilities (RFID systems). The marketability of the patent solution was tested in Finland without a positive feed-back.
	Šifra		F.33 Patent v Sloveniji
	Objavljeno v		Patent št. 22773, UIL Republike Slovenije, 2008
	Tipologija		2.24 Patent
	COBISS.SI-ID		1024179796
4.	Naslov	*SLO*	D. Kovač, Obvladovanje zaupanja v storitveno usmerjenih arhitekturah, doktorska disertacija
		ANG	D. Kovač, Trust management in SOA, PhD Thesis
	Opis	*SLO*	Ta doktorat podaja razširjen formalni model, metodologijo in tehnološke rešitve za obvladovanje zaupanja v storitveno usmerjenih arhitekturah, ki predstavlja pomembno nadgradnjo raziskav v Laboratoriju za e-medije FRI UL.
		ANG	This Ph.D. thesis presents extended formal model, methodology and technological solution for trust management in SOA environments, with important contributions that further upgrade research done so far in Laboratory of e-media at FRI UL.
	Šifra		D.09 Mentorstvo doktorandom
	Objavljeno v		DIGKUL
	Tipologija		4.00 Sekundarno avtorstvo
	COBISS.SI-ID		7268180
5.	Naslov	*SLO*	D. Trček, G. Božič, Sadovi znanja
		ANG	D. Trček, G. Božič, Sadovi znanja
	Opis	*SLO*	Ta TV oddaja opisuje raziskave projekta LaKS in popularizira raziskave na omenjenem področju.
		ANG	This TV clip gives a presentation of the LaKS project and popularizes the related field of science.
	Šifra		B.04 Vabljeno predavanje
	Objavljeno v		POP TV
	Tipologija		2.19 Radijska ali televizijska oddaja
	COBISS.SI-ID		7110228

8. Drugi pomembni rezultati projetne skupine[7]

Na podlagi dodatnih rezultatov pri kvantitativnem obvladovanju tveganj smo s Stanford University prijavili projekt pri US Dept. of Homeland Security.

9. Pomen raziskovalnih rezultatov projektne skupine[8]

9.1. Pomen za razvoj znanosti[9]

SLO

Pomen projekta za razvoj znanosti je sledeč:

Razvoj metodologije za kvantitativno vrednotenje »lahkosti« kriptografskih protokolov, ki pa je nato pripeljala do dodatnega preboja z metodologijo za kvantitativno obvladovanje tveganj v informacijskih sistemih (glej Computer Journal, Oxford Uni-Press). Tu orjemo ledino in to delo nas je pripeljalo v en konzorcij za prijavo projekta 7 OP EU.

Drug pomemben prispevek pa je nova metodologija za obvladovanje zaupanja, imenovana kvalitativna algebra. Ta formalizem pravzaprav izhaja s področja psihologije in je komplementaren k pristopom, ki temeljijo na racionalnih igralcih (npr. Dempster-Shaferjeva teorija evidence in teorija iger). Kvalitativna algebra omogoča modeliranje uporabnikov in njihovo podporo v okoljih vseprisotnega računalništva (pa tudi širše) izhajajoč iz lingvistično-izkustvenih osnov, ki služijo kot temelj za določanje obnašanja agentov in sprejemanje odločitev. Tudi ta metodologija je že bila objavljena v reviji SCI (glej Mathematical & Computer Modeling, Elsevier, 2008).

ANG

The importance of the project for science:

Development of a methodology for measurement of »lightweightness« of a cryptographic protocols. This methodology further led to considerable advancement with a methodology for quantitative risks management in information systems (see Computer Journal, Oxford Uni-Press). Here we were doing a pioneering research that will enable tangible assessment (reactive, active and proactive) of risks, and this work resulted in our membership in one consortium for FW 7 project.

Another important contribution is new methodology called qualitative algebra. This formalism is aimed at trust management and presents a complementary to those based on rational players (e.g. Dempster-Shafer theory of evidence and game theory). Qualitative algebra allows modeling users and their support in pervasive computing environments to enable better decision making. It is based on linguistic-experiences approach to determine behavior of agents and their decision. The methodology has already been published in SCI journal (see Mathematical & Computer Modeling, Elsevier, 2008).

9.2. Pomen za razvoj Slovenije[10]

SLO

Na osnovi opravljenega raziskovalnega dela v okviru projektu LaKS smo bili vabljeni v programske odbore mnogih mednarodnih znanstvenih konferenc (IEEE WSSP 09, Los Angeles, ACM Workshop on Secure Web Services 09, Chicago,…). Dobili smo dve vabili za uvodni vabljeni predavanji na mednarodnih znanstvenih konferencah AIC'08 in AIC'09. Nadalje smo bili povabljeni v dva konzorcija za projekte v okviru EU in na eni od prijav tudi uspeli (projekt SEMPOC). To pomeni, da smo iz evropskih sredstev financirali in zaposlili nove raziskovalce, ki bodo opravljali delo, relevantno za EU in tudi Slovenijo (na področju varovanja kritičnih infrastruktur). Dobili smo tudi nagrado za najboljši članek na konferenci IARIA ICONS 2009 .

Sami rezultati, ki so dosegljivi v COBISS-u potrjujejo, da opravljene raziskave ustrezno promovirajo Slovenijo v evropskem in svetovnem prostoru. Imajo pa tudi neposredne pozitivne finančne učinke za Slovenijo samo, saj izobražujemo naše ljudi na področju naprednih raziskav, ki so za to delo 70% plačani iz sredstev EU (ob nekoliko drugačni sistemski ureditvi v Sloveniji bi bili sposobni akumulirati še več denarja iz EU).

ANG

Based on the results of our research within LaKS project we were invited to many program committees of international scientific conferences (IEEE WSSP 09, Los Angeles, ACM Workshop on Secure Web Services 09, Chicago,…). We also received an invitation for a presentation at AIC'08 and AIC'09. Furthermore, we were invited into two consortia for EU projects and we succeeded to get one (SEMPOC). This means that we will be able to finance (and employ) new young researchers that will do new research for the benefit of Slovenia and EU (in the area of protection of critical infrastructures). Last but not least, we have been awarded best paper award at IARIA ICONS 2009 conference.

The results (all of them are documented in COBISS) prove that our research promotes Slovene science in the EU and worldwide. But it has also clear positive financial implications for the local environment.

10. Samo za aplikativne projekte!
Označite, katerega od navedenih ciljev ste si zastavili pri aplikativnem projektu, katere konkretne rezultate ste dosegli in v kakšni meri so doseženi rezultati uporabljeni

Cilj		
F.01	**Pridobitev novih praktičnih znanj, informacij in veščin**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	
F.02	**Pridobitev novih znanstvenih spoznanj**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	
F.03	**Večja usposobljenost raziskovalno-razvojnega osebja**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	
F.04	**Dvig tehnološke ravni**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	
F.05	**Sposobnost za začetek novega tehnološkega razvoja**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	
F.06	**Razvoj novega izdelka**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	
F.07	**Izboljšanje obstoječega izdelka**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	
F.08	**Razvoj in izdelava prototipa**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	
F.09	**Razvoj novega tehnološkega procesa oz. tehnologije**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	

	Uporaba rezultatov	
F.10	**Izboljšanje obstoječega tehnološkega procesa oz. tehnologije**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.11	**Razvoj nove storitve**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.12	**Izboljšanje obstoječe storitve**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.13	**Razvoj novih proizvodnih metod in instrumentov oz. proizvodnih procesov**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.14	**Izboljšanje obstoječih proizvodnih metod in instrumentov oz. proizvodnih procesov**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.15	**Razvoj novega informacijskega sistema/podatkovnih baz**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.16	**Izboljšanje obstoječega informacijskega sistema/podatkovnih baz**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.17	**Prenos obstoječih tehnologij, znanj, metod in postopkov v prakso**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.18	**Posredovanje novih znanj neposrednim uporabnikom (seminarji, forumi, konference)**	
	Zastavljen cilj	DA NE
	Rezultat	

	Uporaba rezultatov	
F.19	**Znanje, ki vodi k ustanovitvi novega podjetja ("spin off")**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.20	**Ustanovitev novega podjetja ("spin off")**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.21	**Razvoj novih zdravstvenih/diagnostičnih metod/postopkov**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.22	**Izboljšanje obstoječih zdravstvenih/diagnostičnih metod/postopkov**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.23	**Razvoj novih sistemskih, normativnih, programskih in metodoloških rešitev**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.24	**Izboljšanje obstoječih sistemskih, normativnih, programskih in metodoloških rešitev**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.25	**Razvoj novih organizacijskih in upravljavskih rešitev**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.26	**Izboljšanje obstoječih organizacijskih in upravljavskih rešitev**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.27	**Prispevek k ohranjanju/varovanje naravne in kulturne dediščine**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.28	**Priprava/organizacija razstave**	

	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	
F.29	**Prispevek k razvoju nacionalne kulturne identitete**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	
F.30	**Strokovna ocena stanja**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	
F.31	**Razvoj standardov**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	
F.32	**Mednarodni patent**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	
F.33	**Patent v Sloveniji**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	
F.34	**Svetovalna dejavnost**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	
F.35	**Drugo**	
	Zastavljen cilj	○ DA ○ NE
	Rezultat	
	Uporaba rezultatov	

Komentar

11. Samo za aplikativne projekte!
Označite potencialne vplive oziroma učinke vaših rezultatov na navedena področja

	Vpliv	**Ni vpliva**	**Majhen vpliv**	**Srednji vpliv**	**Velik vpliv**	

G.01	**Razvoj visoko-šolskega izobraževanja**					
G.01.01.	Razvoj dodiplomskega izobraževanja	○	○	○	○	
G.01.02.	Razvoj podiplomskega izobraževanja	○	○	○	○	
G.01.03.	Drugo:	○	○	○	○	
G.02	**Gospodarski razvoj**					
G.02.01	Razširitev ponudbe novih izdelkov/storitev na trgu	○	○	○	○	
G.02.02.	Širitev obstoječih trgov	○	○	○	○	
G.02.03.	Znižanje stroškov proizvodnje	○	○	○	○	
G.02.04.	Zmanjšanje porabe materialov in energije	○	○	○	○	
G.02.05.	Razširitev področja dejavnosti	○	○	○	○	
G.02.06.	Večja konkurenčna sposobnost	○	○	○	○	
G.02.07.	Večji delež izvoza	○	○	○	○	
G.02.08.	Povečanje dobička	○	○	○	○	
G.02.09.	Nova delovna mesta	○	○	○	○	
G.02.10.	Dvig izobrazbene strukture zaposlenih	○	○	○	○	
G.02.11.	Nov investicijski zagon	○	○	○	○	
G.02.12.	Drugo:	○	○	○	○	
G.03	**Tehnološki razvoj**					
G.03.01.	Tehnološka razširitev/posodobitev dejavnosti	○	○	○	○	
G.03.02.	Tehnološko prestrukturiranje dejavnosti	○	○	○	○	
G.03.03.	Uvajanje novih tehnologij	○	○	○	○	
G.03.04.	Drugo:	○	○	○	○	
G.04	**Družbeni razvoj**					
G.04.01	Dvig kvalitete življenja	○	○	○	○	
G.04.02.	Izboljšanje vodenja in upravljanja	○	○	○	○	
G.04.03.	Izboljšanje delovanja administracije in javne uprave	○	○	○	○	
G.04.04.	Razvoj socialnih dejavnosti	○	○	○	○	
G.04.05.	Razvoj civilne družbe	○	○	○	○	
G.04.06.	Drugo:	○	○	○	○	
G.05.	**Ohranjanje in razvoj nacionalne naravne in kulturne dediščine in identitete**	○	○	○	○	
G.06.	**Varovanje okolja in trajnostni razvoj**	○	○	○	○	
G.07	**Razvoj družbene infrastrukture**					
G.07.01.	Informacijsko-komunikacijska infrastruktura	○	○	○	○	
G.07.02.	Prometna infrastruktura	○	○	○	○	
G.07.03.	Energetska infrastruktura	○	○	○	○	
G.07.04.	Drugo:	○	○	○	○	

G.08.	**Varovanje zdravja in razvoj zdravstvenega varstva**	○	○	○	○	
G.09.	**Drugo:**	○	○	○	○	

Komentar

12. Pomen raziskovanja za sofinancerje, navedene v 2. točki[11]

1.	**Sofinancer**			
	Vrednost sofinanciranja za celotno obdobje trajanja projekta je znašala:			**EUR**
	Odstotek od utemeljenih stroškov projekta:			**%**
	Najpomembnejši rezultati raziskovanja za sofinancerja			**Šifra**
		1.		
		2.		
		3.		
		4.		
		5.		
	Komentar			
	Ocena			
2.	**Sofinancer**			
	Vrednost sofinanciranja za celotno obdobje trajanja projekta je znašala:			**EUR**
	Odstotek od utemeljenih stroškov projekta:			**%**
	Najpomembnejši rezultati raziskovanja za sofinancerja			**Šifra**
		1.		
		2.		
		3.		
		4.		
		5.		
	Komentar			
	Ocena			
3.	**Sofinancer**			
	Vrednost sofinanciranja za celotno obdobje trajanja projekta je znašala:			**EUR**

Odstotek od utemeljenih stroškov projekta:			**%**
Najpomembnejši rezultati raziskovanja za sofinancerja			**Šifra**
	1.		
	2.		
	3.		
	4.		
	5.		
Komentar			
Ocena			

C. IZJAVE

Podpisani izjavljam/o, da:

- so vsi podatki, ki jih navajamo v poročilu, resnični in točni
- se strinjamo z obdelavo podatkov v skladu z zakonodajo o varstvu osebnih podatkov za potrebe ocenjevanja, za objavo 6., 7. in 8. točke na spletni strani http://sicris.izum.si/ ter obdelavo teh podatkov za evidence ARRS
- so vsi podatki v obrazcu v elektronski obliki identični podatkom v obrazcu v pisni obliki
- so z vsebino zaključnega poročila seznanjeni in se strinjajo vsi soizvajalci projekta

Podpisi:

Roman Novak	in	
podpis vodje raziskovalnega projekta		zastopnik oz. pooblaščena oseba RO

Kraj in datum:	Ljubljana	6.4.2010

Oznaka poročila: ARRS-RPROJ-ZP-2010-1/57

---

[1] Samo za aplikativne projekte. Nazaj

[2] Napišite kratko vsebinsko poročilo, kjer boste predstavili raziskovalno hipotezo in opis raziskovanja. Navedite ključne ugotovitve, znanstvena spoznanja ter rezultate in učinke raziskovalnega projekta. Največ 18.000 znakov vključno s presledki (približno tri strani, velikosti pisave 11). Nazaj

[3] Realizacija raziskovalne hipoteze. Največ 3.000 znakov vključno s presledki (približno pol strani, velikosti pisave 11). Nazaj

[4] Samo v primeru bistvenih odstopanj in sprememb od predvidenega programa raziskovalnega projekta, kot je bil zapisan v predlogu raziskovalnega projekta. Največ 3.000 znakov vključno s presledki (približno pol strani, velikosti pisave 11). Nazaj

[5] Navedite največ pet najpomembnejših znanstvenih rezultatov projektne skupine, ki so nastali v času trajanja projekta v okviru raziskovalnega projekta, ki je predmet poročanja. Za vsak rezultat navedite naslov v slovenskem in angleškem jeziku (največ 150 znakov vključno s presledki), rezultat opišite (največ 600 znakov vključno s presledki) v slovenskem in angleškem jeziku, navedite, kje je objavljen (največ 500 znakov vključno s presledki), izberite ustrezno šifro tipa objave po Tipologiji dokumentov/del za vodenje bibliografij v sistemu COBISS ter napišite ustrezno COBISS.SI-ID številko bibliografske enote.
Navedeni rezultati bodo objavljeni na spletni strani http://sicris.izum.si/.

PRIMER (v slovenskem jeziku):
Naslov: Regulacija delovanja beta-2 integrinskih receptorjev s katepsinom X;
Opis: Cisteinske proteaze imajo pomembno vlogo pri nastanku in napredovanju raka. Zadnje študije kažejo njihovo povezanost s procesi celičnega signaliziranja in imunskega odziva. V tem znanstvenem članku smo prvi dokazali… (največ 600 znakov vključno s presledki)
Objavljeno v: OBERMAJER, N., PREMZL, A., ZAVAŠNIK-BERGANT, T., TURK, B., KOS, J.. Carboxypeptidase cathepsin X mediates ß2 - integrin dependent adhesion of differentiated U-937 cells. Exp. Cell Res., 2006, 312, 2515-2527, JCR IF (2005): 4.148
Tipopologija: 1.01 - Izvirni znanstveni članek
COBISS.SI-ID: 1920113 Nazaj

[6] Navedite največ pet najpomembnejših družbeno-ekonomsko relevantnih rezultatov projektne skupine, ki so nastali v času trajanja projekta v okviru raziskovalnega projekta, ki je predmet poročanja. Za vsak rezultat navedite naslov (največ 150 znakov vključno s presledki), rezultat opišite (največ 600 znakov vključno s presledki), izberite ustrezen rezultat, ki je v Šifrantu raziskovalnih rezultatov in učinkov (Glej: http://www.arrs.gov.si/sl/gradivo/sifranti/sif-razisk-rezult.asp), navedite, kje je rezultat objavljen (največ 500 znakov vključno s presledki), izberite ustrezno šifro tipa objave po Tipologiji dokumentov/del za vodenje bibliografij v sistemu COBISS ter napišite ustrezno COBISS.SI-ID številko bibliografske enote.
Navedeni rezultati bodo objavljeni na spletni strani http://sicris.izum.si/. Nazaj

[7] Navedite rezultate raziskovalnega projekta v primeru, da katerega od rezultatov ni mogoče navesti v točkah 6 in 7 (npr. ker se ga v sistemu COBISS ne vodi). Največ 2.000 znakov vključno s presledki. Nazaj

[8] Pomen raziskovalnih rezultatov za razvoj znanosti in za razvoj Slovenije bo objavljen na spletni strani: http://sicris.izum.si/ za posamezen projekt, ki je predmet poročanja. Nazaj

[9] Največ 4.000 znakov vključno s presledki Nazaj

[10] Največ 4.000 znakov vključno s presledki Nazaj

[11] Rubrike izpolnite/prepišite skladno z obrazcem "Izjava sofinancerja" (http://www.arrs.gov.si/sl/progproj/rproj/gradivo/), ki ga mora izpolniti sofinancer. Podpisan obrazec "Izjava sofinancerja" pridobi in hrani nosilna raziskovalna organizacija – izvajalka projekta. Nazaj

Obrazec: ARRS-RPROJ-ZP/2010 v1.00
F9-05-DD-6F-43-28-1C-6B-85-3F-C1-38-A9-67-C0-D7-C1-33-71-73