Projekat 0274:

SOFTVERSKI SISTEM ZA ZAŠTIĆENO ELEKTRONSKO ARHIVIRANJE

Elaborat

o realizaciji i rezultatima projekta tokom 2002. - 2004. godine

rukovodilac projekta

Dr Miodrag Mihaljević, naučni savetnik

Matematički institut SANU

Abstract

Ovaj elaborat tipa preglednog rada daje prikaz realizacije i rezultata projekta tehnološkog razvoja 0274 "Softverski sistem za zaštićeno elektronsko arhiviranje" tokom 2002., 2003. i 2004. godine. Osnovni rezultat projekta je razvoj softverskog sistema za zaštićeno elektronsko arhiviranje sa mehanizmima za kriptografsku zaštitu podataka u WINDOWS okruženju, fleksibilnih karakteristika, pogodnog za primenu u oblasti elektronskog poslovanja, elektronske državne uprave i elektronskog zdravstva. Tokom tri godine projekat je finansiran sa ukupno 72 istrazivac meseca tokom kojih je realizovano: (i) jedan softverski sistem; (ii) 7 softverskih podistema; (iii) 2 studije i dva projekta; (iV) 3 rada publikovana u medjunarodnim časopisima; (v) 15 publikovanih radova razlicitih kategorija. Istice se da je projekat od direktnog znacaja (interesa) za razvoj "informatickog drustva" ukljucujuci "e-government", "e-commerce", "e-business", ... Realizacija projekta je ostvarila sve planirane ciljeve a na osnovu dodatnih aktivnosti postignuto je da ukupni rezultati projekta i po kvantitetu i po kvalitetu značajno nadmašuju inicijalno planirane izlazne rezultate.

Matematički institut SANU, Beograd

januar 2005. godine

1 Uvod

- *Predmet istraživanja*:
  Predmet istraživanja i razvoja su nove realizacije za bezbedno arhiviranje i dalju upotrebu informacija u formi računarskih podataka. Razvija se softverski sistem za elektronsko arhiviranje sa mehanizmima za kriptografku zastitu podataka. Sistem se razvija za WINDOWS okruzenje uz zahteve za visokom efikasnošću i jednostavnom upotrebom. Planirane aplikacije rezultata istraživanja i razvoja su u domenima elektronskog poslovanja, elektronske državne uprave i elektronskog zdravstva.

- *Sadržaj istraživanja*:
  Polazeći od najnovijih rezultata u oblasti, dizajnira se i implementira softverski sistem sa fleksibilnim karakteristikama pogodan za različite aplikacije vezane za elektronsko arhiviranje.

  Osnovne komponente planiranih istraživačko-razvojnih aktivnosti obuhvataju sledeće:
  - analiza postojećih rešenja i specifičnih zahteva
  - idejno rešenje celine sistema i podsistema
  - projekat sistema i podsistema
  - konstrukcija specijalnih algoritama
  - implementacija autonomnih podsistema
  - implementacija sistema bez autonomnih podsistema
  - integracija podsistema u sistem i testiranja
  - evaluacija sistema.

  Posebno se ističe da sadržaj istraživanja obuhvata i konstrukciju novih specijalnih postupaka za zaštitu tajnosti podataka i proveru njihove sigurnosti. Ovi postupci su komponente odgovarajućih kriptografskih podsistema koji uključuju i izbor kvalitetnih i efikasnih kriptografskih tehnika objavljenih u javnoj literaturi. Kombinacija novih, prilagodjenih tehnika sa tradicionalnim (u upotrebi) obezbedjuje ostvarivanje prilagodjene specifičnosti ("kastomizacija") sa jedne strane i široku kompatibilnost sa druge strane. Komponente sistema su i prilagodjeni protokoli sa smart-karticama koji podržavaju efikasnost i fleksibilnost sistema.

- *Cilj istraživanja*:
  Izrada softverskog sistema za zaštićeno elektronsko arhiviranje sa mehanizmima za kriptografsku zaštitu podataka u WINDOWS okruženju, fleksibilnih karakteristika, pogodnog za primenu u oblasti elektronskog poslovanja, elektronske državne uprave i elektronskog zdravstva.

- *Značaj projekta*:
  Istice se da je projekat od direktnog znacaja (interesa) za razvoj "informatickog drustva" ukljucujuci "e-government", "e-commerce", "e-business", ... Takodje se napominje da EU FP6 (Framework Program 6) kao jedan od prioritetnih pravaca istice projekte vezane za "informaticko drustvo" (Information Society Technologies - IST) stimulisuci ove projete sa jednim od najvecih budzeta.

- *Organizacija Elaborata*. U odeljku 2 dat je pregled i sumarna ocena realizacije projekta. Odeljak 3 prikazuje ciljeve i ostvarene rezultate po godinama realizacije. Ilustrativni rezultati projkta su prikazani u odeljku 4, lista svih rezultata projekta organizovana po tipu ostvarenih rezultata je data u odeljku 5.

2 Pregled i sumarna ocena realizacije projekta

2.1 Pregled realizacije projekta

Sledeća tabela daje sumarni pregled aktivnosti i ostvarenih rezultata tokom realizacije projekta 0274.

Tabela I: Sumarni pregled realizovanih aktivnosti i ostvarenih rezultata

Faze realizacije i godine	*Aktivnosti*	*Rezultati*
I. Projekat sistema 2002.	1. Prethodna analiza za dizajn sistema 2. Projekat sistema	1 studija 1 projekat
II. Projekti podsistema 2002.	1. Prethodna analiza za dizajn podsistema 2. Projekti podsistema	1 studija 1 projekat
III. Algoritmi, Protokoli Aplikacije, Implementacije 2003.	1. Elementi za evaluaciju zaštite tajnosti 2. Korišćeni i potencijalno relevantni protokoli 3. Aplikaciona i implementaciona pitanja	5 objavljenh radova
IV. Implementacija Sistema 2003.	1. Izrada softvera sistema bez podsistema 2. Evaluacija i korekcija softvera	1 softver 1 softver
V. Implementacija Podistema 2003.	1. Izrada softvera podsistema za Digitalni potpis (integritet/autentičnost) 2. Evaluacija i korekcija softvera	5 softvera 5 softvera
VI. Algoritmi, Protokoli Aplikacije, Implementacije 2003.	1. Novi algoritm za zaštitu tajnosti 2. Korišćeni i potencijalno relevantni protokoli 3. Aplikaciona i implementaciona pitanja	3 objavljena rada
VII. Novi metod za Zaštita tajnosti 2004.	1. Izrada softvera podsistema za zaštitu tajnosti 2. Evaluacija i korekcija softvera	1 softver 1 softver
VIII. Integracija sistema 2004.	1. Integracija softvera celine sistema i podsistema 2. Evaluacija i korekcija softvera	2 softvera 2 softvera
IX. Algoritmi, Protokoli Aplikacije, Implementacije 2004.	1. Metodi za evaluaciju kriptografske sigurnosti 2. Korisceni i potencijalno relevantni protokoli 3. Aplikaciona i implementaciona pitanja	9 objavljenih radova

2.2 Obim finansiranja i angažovani istraživači

Projekat je finansiran sa ukupno 72 istrazivač meseca tokom tri godine.

Projekat je realizovao sledeći istraživački tim (svi članovi tima su bili angažovani sa po 4 meseca godišnje):

1. Dr Miodrag Mihaljević, naučni savetnik
2. Dr Zoran Marković, viši naučni saradnik
3. Dr Dragan Blagojević, naučni saradnik
4. Dr Milan Marković, naučni saradnik
5. Dr Dragan Urošević, istraživač saradnik
6. Mr Dejan Bajić, istraživač saradnik

Posebno se ističe da je projekat realizovan sa ne-finansiranim direktnim materijalnim troškovima.

2.3 Sumarna ocena realizacije projekta

Projekat je realizovan u punoj saglasnosti sa ugovornim planom realizacije koji je definisao pravce istrazivanja. Sa druge strane, realizovan je i niz aktivnosti i ostvareni su rezultati koji nisu bili inicijalno planirani. Sumarno posmatrano, ukupni ostvareni rezultati nadmasuju planirani obim ocekivanih rezultata i po kvantitetu i po kvalitetu.

Ukazuje se da faze projekta III, VI i IX navedene u Tabeli I, u sustini nisu bile inicijalno planirane a rezultovale su u objavljivanju ukupno 15 radova od čega 3 rada u medjunarodnim časopisima, jedno poglavlje u monografiji, 1 rad u nacionalno časopisu, i 6 radova na medjunarodnim naučnim skupovima.

Sa druge strane, Projekat je tokom svake od 3 godine finansiran sa ukupno 24 "istrazivac-meseci" ili 2 "istrazivac-godina", sto znaci da je, u proseku, svaka finansirana istrazivac-godina dala vise od 5 rezultata tipa tehničkog rešenja ili publikovanog rada.

Saglasno svemu navedenom nedvosmisleno je da je realizacija projekta bila veoma uspesna i značajno nadmašila inicijalno planirane izlazne rezultate.

3 Rezime realizacije projekta po godinama

Rezime realizacije projekta po godinama je sledeći.

3.1 Godina 2002.

Rezultati rada na Projektu 0274 tokom 2002. godine su uobliceni u formi 4 studije-elaborata, jednog rada objavljenog u inostranom strucnom casopisu, dva rada na medjunarodnim konferencijama i dva rada na nacionalnim konferencijama.

Ciljevi istrazivanja u prvoj godini su bili: (a) prethodna analiza postojecih rezultata od interesa za ostvarivanje konacnog cilja projekta; (b) projekat celine i podsistema softverskog sistema za zasticeno elektronsko arhiviranje.

Cilj (a) je ostvaren kroz sledece rezultate (koji uključuju i rezultate faze III iz Tabele I):

- "Prethodna analiza za dizajn softverskog sistema za zastiticeno elektronsko arhiviranje".

- "Prethodna analiza za dizajn podsistema softverskog sistema za zasticeno elektronsko arhiviranje".

- "Security evaluation of stream ciphers", Computer Today (Japan), vol. 107, pp. 4-10, 2002.

- "RSA algorithm optimization on assembler of TI TMS320C54x signal processors," EUSIPCO 2002, Toulouse, France, Sept. 3-6, 2002.

- "Cryptographic Techniques and Security Protocols in Modern TCP/IP Computer Networks," Short-Tutorial, ICEST 2002, Oct., 1-4, 2002.

- "O poboljsanju efikasnosti implementacije RSA algoritma na TMS320C54x signal procesorima," Zbornik radova YU INFO 2002, Kopaonik, 2002.

- "O mogucim efikasnim realizacijama AES algoritma na signal procesorima TI TMS320C54x familije," Zbornik radova XLVI Konf. ETRAN, Banja Vrucica, Teslic, 4-7 juni 2002, tom 1, str. 122-125, 2002.

Cilj (b) je ostvaren kroz sledece rezultate:

- "Projekat softverskog sistema za zasticeno elektronsko arhiviranje".

- "Projekat podsistema softverskog sistema za zasticeno elektronsko arhiviranje".

3.2 Godina 2003.

Na osnovu izradjenog projeta celine i podistema softverskog sistema za zasticeno elektronsko arhiviranje (realizovanog tokom prve godine rada) cilj rada u drugoj godini je bio razvoj navedenim projektima specificiranih softvera. Razvijanje ovih softvera je realizovano na osnovu javno dostupnih kriptografskih algoritama. Sa druge strane, jedna od karakteristika rada tokom trece godine obuhvatila je implementaciju i jednog novog kriptografskih algoritama, a finalna aktivnost je obuhvatila i evaluaciju celine softverskog sistema sa novim kriptografskim algoritmima.

Saglasno navedenom, osnovne aktivnosti tokom 2003. godine su bile:

- Izrada softvera sistema bez podsistema; evaluacija i korekcija softvera;

- Izrada softvera podsistema za integritet i autenticnost; evaluacija i korekcija softvera;

- Izrada softvera podsistema za zastitu tajnosti; evaluacija i korekcija softvera;

- Izrada softvera eDocSecure podsistema (interfejs za arhiviranje pojedinacnih dokumenata); evaluacija i korekcija softvera;

- Izrada softvera eDocSecureCentral podsistema (sofver arhivskog centra); evaluacija i korekcija softvera;

- Izrada podsistema Certifikacionog tela; evaluacija i korekcija softvera;

- konstrukcija novog algoritma za zaštitu tajnosti podataka.

Navedeni ciljevi su u potpunosti ostvareni kroz sledeće rezultate:

- "Softver sistema bez podsistema za zatieno elektronsko arhiviranje", Mat. Inst. SANU, Beograd, dec. 2003.

- "Softver podsistema za integritet i autenticnost za zastieno elektronsko arhiviranje", Mat. Inst. SANU, Beograd, dec. 2003.

- "Softver podsistema za zastitu tajnosti za zasticeno elektronsko arhiviranje", Mat. Inst. SANU, Beograd, dec. 2003.

- "Softver interfejs za arhiviranje pojedinacnih dokumenata za zasticeno elektronsko arhiviranje", Mat. Inst. SANU, Beograd, dec. 2003.
- "Softver arhivskog centra za zasticeno elektronsko arhiviranje", Mat. Inst. SANU, Beograd, dec. 2003.
- "Softver podsistema certifikacionog tela za zasticeno elektronsko arhiviranje", Mat. Inst. SANU, Beograd, dec. 2003.
- "On vulnerabilities and improvements of Fast Encryption Algorithm for Multimedia FEA-M", IEEE Trans. Cons. Electr., vol. 49, no. 4, pp. 1199-1207, Nov. 2003.

Tokom 2003. godine realizovana je i dodatna aktivnost "Algoritmi, protokoli, aplikacije i implementacije" koja je rezultovala u objavljivanju sledećih radova:

- "Development of Secure Web Financial Services in Serbia", Information Security Solutions Europe - ISSE 2003, Oct. 7-10, 2003.
- "On optimizing RSA algorithm implementation on signal processor regarding asymmetric private key length", WISP 2003, Sept. 2003, Budapest, Hungary, Proceedings, pp. 73-78, 2003.

3.3 Godina 2004.

Osnovni istraživačko razvojni ciljevi u 2004. godini su bili sledeći

osnovni ciljevi

- Izrada softvera podsistema za zaštitu tajnosti na osnovu novorazvijenog algoritma u 2003. godini; Evaluacija i korekcija softvera;
- Integracija softverskog sistema: Evaluacija i korekcija softvera;

i sledeći dodatni cilj

- Elementi algoritama, protokola, aplikacija i implementacija relevantnih za projekat.

Navedeni ciljevi su u potpunosti ostvareni kroz sledeće osnovne rezultate

- "Improved-FEA-M - Softver II podsistema za zastitu tajnosti za zasticeno elektronsko arhiviranje: Implementacija novog algoritma za sifrovanje/desifrovanje", Mat. Inst. SANU, Beograd, dec. 2004.
- "eEDocSecure - Softver sistema za zasticeno elektronsko arhiviranje, 1.10", Mat. Inst. SANU, Beograd, dec. 2004
- "eEDocSecure-MISANU - Softver sistema za zasticeno elektronsko arhiviranje, 1.24", Mat. Inst. SANU, Beograd, dec. 2004

i sledeće dodatne rezultate

- "Reconfigurable key management for broadcast encryption", IEEE Communications Letters, vol. 8, pp. 440-442, July 2004
- "Tehnike zastite i kriptografski protokoli u savremenim informacionim sistemima", InfoM Casopis, 9/2003, str. 4-13, 2004.
- "Secure mobile health systems: Principles and solutions", in M-Health: Emerging Mobile Health Systems, Robert H. Istepanian, Swamy Laxminarayan and Constantinos S. Pattichis, Editors, Kluwer Academic/Plenum Publishers, (accepted for publication, 2004).
- "Framework of a novel technique for algebraic and fast correlation attacks based on dedicated sample decimation", The State of the Art of Stream Ciphers - SASC 2004, Bruge, Belgium, October 2004, Workshop Record, pp. 190-201.
- "One-way mapping of keys and the overheads trade-off in key management schemes for broadcast encryption", Int. Symp. Inform. Theory and its Appl. - ISITA2004, Parma, Italy, October 2004, Proceedings, pp. 486-491.
- "A method for data access control in certain storage area networks", 7th Int. Symp. on Wireless Personal Multimedia Comm. - WPMC2004, Abano Terme, Italy, September 2004, Proceedings, pp.V3:488-491.
- "Recent PKI experiences in Serbia", in Proceedings of Information Security Solutions Europe - ISSE 2004, September 28-30, 2004, Berlin, and also in ISSE 2004 Securing Electronic Business Processes, Highlights of the ISSE 2004 Conference, Sachar Paulus, Norber Pohlman, Helmut Reimer, Eds., pp. 321-332.
- "Zakon o elektronskom potpisu i podzakonska akta: Kriterijumi za izdavanje kvalifikovanih elektronskih sertifikata", rad po pozivu, Infoteh 2004.
- "Kriterijumi za formiranje kvalifikovanih elektronskih potpisa i izdavanje kvalifikovanih sertifikata", rad po pozivu, IS DOS 2004.
- "EMV tehnologija u prevenciji zloupotreba platnih kartica", rad po pozivu, Savetovanje Prevencija i zastita od zloupotreba platnih kartica, Privredna Komora Srbije, 10. jun 2004.

4 Prikaz ilustrativnih rezultata projekta

4.1 Izabrani osnovni rezultati projeka

4.1.1 Softver "eDocSecure-MISANU"

Softver "eDocSecure-MISANU" je centralni rezultat projekta namenjen za zaštitu sadržaja fajlova krajnjih korisnika.

Osnovna funkcija softvera je da obezbedi zaštitu integriteta i tajnosti sadžaja fajla. Na ovaj način je omogućna i neporecivost slanja ovako zaštićenog fajla. Zaštićni fajlovi se mogu

bezbedno čuvati, kao i prenositi svim raspoloživim komunikacionim sredstvima (npr. kao "attach" fajl u elektronskoj poti).

Uvodne napomene

Softver se zasniva na primeni savremenih tehnologija digitalnog potpisivanja, asimetrinih i simetrinih kriptografskih algoritama, i korišćenju smart kartica kao jednog od najbezbednijih medija za čuvanje kriptografskih parametara.

Za rad programa potrebno je:
- instalirati program eDocSecure-MISANU (jednostavnim kopiranjem fajla programa na raunar),
- instalirati odgovarajući čitač smart kartica na računar i odgovarajuće softvere za podršku smart-karticama,
- posedovati vaeću smart karticu.

Svaki korisnik programa treba da poseduje smart karticu na kojoj se nalaze svi potrebni kriptografski parametri jedinstveni za korisnika (par tajnog i javnog kljua duine 1024 bitova, digitalni certifikat). Korisnik je dužan da čuva svoju smart karticu, i da u slučaju otećenja kartice ili druge neispravosti izvrši prijavu nadležnoj službi.

Startovanjem programa, od korisnika se zahteva da se prijavi unošenjem svog korisničkog imena i lozinke, i postavljanjem smart kartice u čitač smart kartica. Posle ispravno izvršene prijave, korisnik ima mogućnost da izvrši digitalno potpisivanje, digitalno potpisivanje i dešifrovanje, verifikaciju potpisa i dešifrovanje, kao i promenu lozinke. U slučaju neke neispravnosti, korisnik se obaveštava o vrsti nastale greške.

Prijava korisnika

Na poetku rada programa korisnik se mora ispravno prijaviti. Potrebno je uneti svoje korisniko ime i lozinku, i postaviti smart karticu u čitač kartica. Dužina korisnikog imena je od 5 do 32 znakova, dok je dužina lozinke od 5 do 16 znakova. Provera unetih podataka i očitavanje smart kartice traje desetak sekundi za koje vreme e biti ispisana poruka "Oitavanje podataka smart kartice u toku ...". Ako se korisnik ispravno predstavio, moći će da nastavi dalji rad, dok se u slučaju da uneti podaci nisu odgovarajući, ispisuje poruka o greški. Treba uzeti u obzir da ukoliko korisnik 3 puta za redom pogreši u unosu imena i lozinke, smart kartica se blokira i više se sa njom ne moe raditi. U tom sluaju kartica se mora vratiti nadležnoj slubi koja će je deblokirati ili izdati novu.

Posle ispravnog predstavljana, korisnik moe nastaviti rad biranjem eljene funkcije. Ako se tokom rada, unese nova smart kartica, na početku izvršavanja bilo koje funkcije, korisnik će biti obavešten da je smart kartica promenjena i zahtevće se prijava sa novom karticom. Zato je potrebno ponoviti funkciju "Login sa drugom karticom" (iz opcije "Kartica" glavnog menija ili izborom odgovarajuće ikonice na "tool bar").

Digitalno potpisivanje fajla

Izborom funkcije "Sign" opcije "File" glavnog menija vrši se digitalno potpisivanje fajla. Zasniva se na primeni asimetričnog kriptografskog algoritma (RSA) sa ključevima duine 1024 bita. Potrebno je izabrati ulazni fajl koji se želi potpisati i navesti ime izlaznog potpisanog

fajla. Ulazni fajl se bira korišćenjem funkcije sa oznakom "Izaberi" u nastavku polja "Ulazni fajl". Fajl se takodje, može i ručno uneti pri ěmu treba upisati punu putanju do fajla. Fajl u koji će se smestiti sadržaj potpisa, takodje se moe birati ili uneti ručno, pri čemu imena ulaznog i izlaznog fajla ne mogu biti ista. Izlaznom fajlu će se inicijalno ponuditi ekstenzija "sig" kojase, po želji, može promeniti.

Funkcija digitalnog potpisivanja se izvršava selekcijom opcije "Potvrdi". Po ispravno završenom potpisivanju pojaviće se poruka o uspešnom procesiranju, dok se u slučaju greške dobija obaveštenje o vrsti nastale greške.

Digitalno potpisivanje i šifrovanje fajla

Izborom funkcije "SignEncrypt" opcije "File" glavnog menija vrši se digitalno potpisivanje i ifrovanje fajla. Zasniva se na primeni asimetrinog kriptografskog algoritma (RSA) sa ključevima dužine 1024 bita i simetričnog kriptografskog algoritma (Improved-FEA-M) sa tajnim ključem dužine 256 bita. Potrebno je izabrati ulazni fajl koji se želi potpisati i šifrovati, i navesti ime izlaznog potpisanog i šifrovanog fajla. Ulazni fajl se bira selekcijom funkcije sa oznakom "Izaberi" u nastavku polja "Ulazni fajl". Fajl se takodje, može i ručno uneti pri čemu treba upisati punu putanju do fajla. Fajl u koji se smešta sadržaj potpisa i ifrata, takodje se moe birati (izborom funkcije sa oznakom "Izaberi" u nastavku polja "Izlazni fajl") ili uneti ručno, pri čemu imena ulaznog i izlaznog fajla ne mogu biti ista. Izlaznom fajlu će se inicijalno ponuditi ekstenzija "enc", a postoji i opcija izbora ekstenzije po elji.

Funkcija digitalnog potpisivanja i šifrovanja se izvrava selektovanjem opcije "Potvrdi". Po ispravno zavrenom potpisivanju i šifrovanju pojaviće se poruka o uspenom procesiranju, dok se u slučaju greške dobija obaveštenje o vrsti nastale greke.

Verifikacija i dešifrovanje fajla

Izborom funkcije "DecryptVerify" i opcije "File" glavnog menija vri se deifrovanje i/ili verifikacija digitalnog potpisa fajla. Zasniva se na primeni simetričnog kriptografskog algoritma (Improved-FEA-M) sa unutrašnjim ključem duine 256 bita i asimetrinog kriptografskog algoritma (RSA) sa ključevima duine 1024 bita.

Program automatski detektuje da li je ulazni fajl koji se obradjuje samo digitalno potpisan ili je potpisan i šifrovan, i na osnovu toga izvršava samo verifikaciju potpisa fajla ili dešifrovanje i verifikaciju potpisa.

Potrebno je izabrati ulazni fajl koji se želi dešifrovati i/ili verifikovati, i navesti ime izlaznog dešifrovanog i/ili potpisanog fajla. Ulazni fajl se bira izborom funkcije sa oznakom "Izaberi" u nastavku polja "Ulazni fajl". Fajl se takodje, može i ručno uneti pri čemu treba upisati punu putanju do fajla. Fajl u koji će se smestiti obradjeni sadržaj, takodje se moe birati (selekcijom funkcije sa oznakom "Izaberi" u nastavku polja "Izlazni fajl") ili uneti ručno, pri čemu imena ulaznog i izlaznog fajla ne mogu biti ista. Izlaznom fajlu se dodaje ekstenzija koju je imao originalni fajl (pre potpisivanja i/ili šiforvanja) i ne može se menjati čak iako se navede drugačija ekstenzija.

Funkcija verifikovanja i/ili deifrovanja se izvršava selekcijom opcije "Potvrdi". Po ispravno završenom verifikovanju i/ili dešifrovanju pojaviće se poruka o uspenom procesiranju,

dok se u slučaju greške obaveštava o vrsti nastale greške.

Promena lozinke korisnika

Izborom funkcije "Promena lozinke" opcija "Kartica" glavnog menija vri se promena lozinke korisnika na smart kartici. Svaki korisnik sa smart karticom, dobija svoje korisničko ime i lozinku kao identifikatore sa kojima se prijavljuje (funkcija "Login") na smart karticu i u program. Korisnik može promeniti svoju lozinku, posle čega se prijavljuje sa novom lozinkom.

Za promenu lozinke potrebno je uneti korisniko ime i tekuću lozinku, kao i novu lozinku. Dužina korisnikog imena je od 5 do 32 znakova, dok je dužina lozinke od 5 do 16 znakova. Novu lozinku je potrebno uneti dva puta da bi se izbegle greške pri unošenju. Iz sigurnosnih razloga, prilikom unošenja lozinke, sadraj lozinke je zamenjem znacima "*".

Funkcija promene lozinke se izvršava selekcijom opcije "Potvrdi". Ovaj postupak traje nekoliko sekundi, za koje vreme se pojavljuje poruka "Promena lozinke u toku". Po ispravno završenoj promeni pojavljuje se poruka o uspešnom radu, dok se u slučaju greške dobija obaveštenje o vrsti nastale greške.

4.1.2 Softver "eDocSecureCental"

Osnovne karakteristike

Softver "eDocSecureCental predstavlja programsku podrku elektronskog delovodje koji vrši elektronsko arhiviranje dokumenata.

Osnovne funkcije programa su da obezbedi:
- proveru autentičnosti potpisnika,
- zaštitu integriteta i
- zaštitu tajnosti sadraja fajla.

Na ovaj način je omogućena i neporecivost slanja ovako zaštićenog fajla. Zatićeni fajlovi se mogu bezbedno čuvati, kao i prenositi svim raspoloživim komunikacionim sredstvima (npr. kao "attach" fajl u elektronskoj poti).

Program eDocSecureCentral se zasniva na primeni savremenih tehnologija digitalnog potpisivanja, asimetričnih i simetričnih kriptolokih algoritama, pri čemu se koristi smart kartica kao jedan od najbezbednijih medija za čuvanje kriptografskih parametara.

"eDocSecureCentral" zajedno sa programima "eDocSecure-MISANU" i "eDocSecure", predstavlja programski sistem za zatićeno elektronsko arhiviranje podataka.

Za ispravan rad programa eDocSecureCentral potrebno je:
- instalirati programski fajl eDocSecureCentral.exe i eDocSecureCentral.hlp (kopiranjem fajlova na računar),
- instalirati biblioteku GSL 3.1 za podrku rada smart kartica,
- instalirati odgovarajući čitač smart kartica na računar,
- posedovati vaeču smart karticu.

Svaki korisnik programa poseduje smart karticu na kojoj se nalaze svi potrebni kriptografski parametri.

Verifikacija integriteta fajla i arhivski potpis

Izborom funkcije "VerifyAndArchive" opcije "File" glavnog menija vri se verifikacija digitalnog potpisa fajla potpisanog programom eDocSecure-MISANU ili eDocSecure i arhivskog potpisa eDocSecureCentral.

Ako arhivski potpis ne postoji moe se uneti delovodni broj i izabrati operacija arhivskog potpisa fajla.

Arhivski digitalni potpis fajlova se zasniva na primeni asimetričnog kriptografskog algoritma (RSA) pri čemu su ključevi duine 1024 bita.

Program automatski detektuje da li je ulazni fajl koji se obradjuje samo digitalno potpisan ili je potpisan i ifrovan, a izvrava samo verifikaciju potpisa fajla.

Arhivaru za sada nije omogučeno da ovim programom dešifruje fajl i dobije originalni dokument. Jedino moe proveriti integritet fajla i izvriti operaciju arhivskog potpisa uz upis delovodnog tekstualnog polja maksimalne duine 60 karaktera čime se realizuje *elektronsko zavodjenje*.

Operacija elektronskog zavodjenja ili verifikovanja kao prvo podrazumeva selekciju ulaznog fajla koji se eli verifikovati i navodjenje imena izlaznog fajla za arhivski potpis.

Ulazni fajl se bira izborom funkcije sa oznakom "Izaberi" u nastavku polja "Ulazni fajl". Fajl se takodje, moe i ručno uneti pri čemu treba upisati punu putanju do fajla. Fajl u koji će se smestiti obradjeni sadraj, takodje se može birati (izborom funkcije sa oznakom "Izaberi" u nastavku polja "Izlazni fajl") ili uneti ručno, pri čemu imena ulaznog i izlaznog fajla ne mogu biti ista.

Ako elimo samo proveru integriteta fajla bez arhivskog potpisivanja potrebno je označiti opciju da se ne pravi izlazni fajl. Funkcija VerifyAndArchive se izvrava izborom opcije "Potvrdi". Po ispravno zavrenom verifikovanju fajla pojaviće se poruka o uspešnom radu, dok se u slučaju greke obavetava o vrsti nastale greške.

Nakon uspešne verifikacije ispisuju se podaci o potpisniku-vlasniku dokumenta i vreme potpisivanja.

Ako je ulazni fajl preuzet iz arhive ispisuju se i delovodni broj dokumenta pod kojim je zaveden u arhivi, potpis arhivara iz eDocSecureCentral i vreme kad je izvren arhivski potpis.

Samo ako nema arhivskog potpisa omogućen je unos delovodnog broja i arhivske oznake dokumenta u tekstualnom polju maksimalne duine 60 karaktera kao i izbor komande Arhivski potpis.

4.1.3 Novi algoritam za šifrovanje/dešifrovanje

Novorazvijeni algoritam za šifrovanje/dešifrovanje je publikovan u sledećoj formi:

- "On vulnerabilities and improvements of Fast Encryption Algorithm for Multimedia FEA-M", IEEE Trans. Cons. Electr., vol. 49, no. 4, pp. 1199-1207, Nov. 2003.

Novorazvijeni algoritam "Improved-FEA-M" je dizajniran na osnovu analize sigurnosti i korekcije detektovanih slabosti algoritma FEA-M koji je publikovan 2001. godine.

Osnova kriptografskog algoritama je bazirana na množenju i sabiranju binarnih matrica i vektora sa svim operacijam nad GF(2).

Analiza kompleksnosti "Improved-FEA-M" merena brojem i prirodom korišćenih aritmetičkih operacija implicira nisku složenost algoritma (zato što je dominantna operacija XOR - sabiranje po modulu 2) podrazumevajuci prilagodjenu i optimiziranu implementaciju.

4.2 Izabrani dodatni rezultati projekta

4.2.1 Prilog metodama za evaluaciju kriptografske sigurnosti jedne klase primitiva za zaštitu tajnosti

Jedan prilog metodama za evaluaciju kriptografske sigurnosti jedne klase primitiva za zaštitu tajnosti je objavljen u formi:

- "Security evaluation of stream ciphers", Computer Today, vol. 107, pp. 4-10, Jan. 2002. (in Japanese).

U navedenom radu sistematizovane su osnovne metode za analizu sigrnosti kriptografskih generatora binarnih pseudoslučajnih nizova. Ove metode su od osnovnog značaja za procenu kriptografske sigurnosti jedne klase kriptografskih primitiva za šifrovanje tipa "stream-ciphers".

4.2.2 Prilog metodama za upravljanje kriptografskim ključevima

Jedan prilog metodama za upravljanje kriptografskim ključevima je objavljen u formi:

- "Reconfigurable key management for broadcast encryption", IEEE Communications Letters, vol. 8, pp. 440-442, July 2004.

U navedenom radu predlozen je koncept dinamičke adaptacije šeme za distribuciju kriptogragfskih ključeva kojim se vrši njeno prilagodjavanje tekućem scenariju distribucije ključeva.

5 Ukupni ostvareni rezultati

Osnovni rezultati projekta 0274 ostvareni tokom 2002., 2003. i 2004. godine.
(List of the Project 0275 Results Achieved in the Years 2002, 2003 and 2004)

- I. Journals - Casopisi:

  [I.1] M. Mihaljevic, "Reconfigurable key management for broadcast encryption", IEEE Communications Letters, vol. 8, pp. 440-442, July 2004. (ISSN: 1089-7798)

  [I.2] M. Mihaljevic, "On vulnerabilities and improvements of Fast Encryption Algorithm for Multimedia FEA-M", IEEE Trans. Cons. Electr., vol. 49, no. 4, pp. 1199-1207, Nov. 2003. (ISSN: 0098-3063)

  [I.3] M. Mihaljevic, Y. Watanabe and H. Imai, "Security evaluation of stream ciphers", Computer Today, vol. 107, pp. 4-10, Jan. 2002. (in Japanese) (ISSN: 0289-3509) (http://www.saiensu.co.jp/CT/stand/0201/sr1.htm)

  [I.4] M.Markovic, "Tehnike zastite i kriptografski protokoli u savremenim informacionim sistemima", InfoM Casopis, 9/2003, str. 4-13. (ISSN 1451-4397, UDC 659.25)

- II. Books (Monographs) - Monografije: Chapters in Books (the Monographs) - Poglavlja u monografijama

  [II.1] M.Markovic, Z.Savic and B.Kovacevic, "Secure mobile health systems: Principles and solutions", in M-Health: Emerging Mobile Health Systems, Robert H. Istepanian, Swamy Laxminarayan and Constantinos S. Pattichis, Editors, Kluwer Academic/Plenum Publishers, (accepted for publication, 2004).

- III. Conference Papers - Skupovi:

  [III.1] M. Mihaljevic and H. Imai, "Framework of a novel technique for algebraic and fast correlation attacks based on dedicated sample decimation", The State of the Art of Stream Ciphers - SASC 2004, Bruge, Belgium, October 2004, Workshop Record, pp. 190-201.

  [III.2] M. Mihaljevic, M.P.C. Fossorier and H. Imai, "One-way mapping of keys and the overheads trade-off in key management schemes for broadcast encryption", Int. Symp. Inform. Theory and its Appl. - ISITA2004, Parma, Italy, October 2004, Proceedings, pp. 486-491. (ISBN: 4-092087-08-1)

  [III.3] M. Mihaljevic and H. Imai, "A method for data access control in certain storage area networks", 7th Int. Symp. on Wireless Personal Multimedia Comm. - WPMC2004, Abano Terme, Italy, September 2004, Proceedings, pp.V3:488-491.

  [III.4] M. Markovic, "Recent PKI experiences in Serbia", in Proceedings of Information Security Solutions Europe - ISSE 2004, September 28-30, 2004, Berlin, and also in ISSE 2004 Securing Electronic Business Processes, Highlights of the ISSE 2004 Conference, Sachar Paulus, Norber Pohlman, Helmut Reimer, Eds., pp. 321-332.

  [III.5] M. Markovic i radna grupa, "Zakon o elektronskom potpisu i podzakonska akta: Kriterijumi za izdavanje kvalifikovanih elektronskih sertifikata", rad po pozivu, Infoteh 2004.

  [III.6] M. Markovic i radna grupa, "Kriterijumi za formiranje kvalifikovanih elektronskih potpisa i izdavanje kvalifikovanih sertifikata", rad po pozivu, IS DOS 2004.

  [III.7] M. Markovic, "EMV tehnologija u prevenciji zloupotreba platnih kartica", rad po pozivu, Savetovanje Prevencija i zastita od zloupotreba platnih kartica, Privredna Komora Srbije, 10. jun 2004.

  [III.8] Z. Savic, M. Markovic, "Development of Secure Web Financial Services in Serbia", Information Security Solutions Europe - ISSE 2003, Oct. 7-10, 2003.

  [III.9] M. Markovic, G. Djordjevic, T. Unkasevic, "On optimizing RSA algorithm implementation on signal processor regarding asymmetric private key length", WISP 2003, Sept. 2003, Budapest, Hungary, Proceedings, pp. 73-78, 2003.

  [III.10] M. Markovic, T. Unkasevic and D. Djordjevic, "RSA algorithm optimization on assembler of TI TMS320C54x signal processors", EUSIPCO 2002, Sept. 3-6, 2002, Toulouse; France, Proceedings, pp. 579 - 582, 2002.

  [III.11] M. Markovic, "Cryptographic Techniques and Security Protocols in Modern TCP/IP Computer Networks" ICEST 2002, Oct. 2002, Nis, Serbia and Montenegro, Proceedings, pp. 23-26, 2002.

  [III.12] G. Djordjevic, M. Markovic, T. Unkasevic, "O poboljsanju efikasnosti implementacije RSA algoritma na TMS320C54x signal procesorima", YU INFO 2002, Kopaonik, Serbia and Montenegro, Zbornik radova, 2002.

[III.13] G. Djordjevc, T. Unkasevic, M. Markovic, "O mogucim efikasnim realizacijama AES algoritma na signal procesorima TI TMS320C54x familije", XLVI Konf. ETRAN, Jun 2002, Banja Vrujci, Serbia and Montenegro, Zbornik radova, str. 122-125, 2002.

- IV. Technical Projects and Softwares - Studije, Projekti, Tehnicka resenja:

  [IV.1] "Prethodna analiza za dizajn softverskog sistema za zastiticeno elektronsko arhiviranje", Editori: M. Markovic, M. Mihaljevic i Z. Markovic, Mat. Inst. SANU, Beograd, 75 strana, jan. 2003.

  [IV.2] "Projekat softverskog sistema za zasticeno elektronsko arhiviranje", Editori: M. Markovic, M. Mihaljevic i Z. Markovic, Mat. Inst. SANU, Beograd, 16 strana, jan. 2003.

  [IV.3] "Prethodna analiza za dizajn podsistema softverskog sistema za zasticeno elektronsko arhiviranje", Editori: M. Markovic, M. Mihaljevic i Z. Markovic, Mat. Inst. SANU, Beograd, 98 strana, jan. 2003.

  [IV.4] "Projekat podsistema softverskog sistema za zasticeno elektronsko arhiviranje", Editori: M. Markovic, M. Mihaljevic i Z. Markovic, Mat. Inst. SANU, Beograd, 48 strana, jan. 2003.

  [IV.5] M. Markovic, D. Bajic, M. Mihaljevic, D. Urosevic, Z. Markovic, D. Blagojevic, "Softver sistema bez podsistema za zatieno elektronsko arhiviranje", Mat. Inst. SANU, Beograd, dec. 2003.

  [IV.6] M. Markovic, D. Bajic, M. Mihaljevic, D. Urosevic, Z. Markovic, D. Blagojevic, "Softver podsistema za integritet i autenticnost za zastieno elektronsko arhiviranje", Mat. Inst. SANU, Beograd, dec. 2003.

  [IV.7] M. Markovic, D. Bajic, M. Mihaljevic, D. Urosevic, Z. Markovic, D. Blagojevic, "Softver podsistema za zastitu tajnosti za zasticeno elektronsko arhiviranje", Mat. Inst. SANU, Beograd, dec. 2003.

  [IV.8] M. Markovic, D. Bajic, M. Mihaljevic, D. Urosevic, Z. Markovic, D. Blagojevic, "Softver interfejs za arhiviranje pojedinacnih dokumenata za zasticeno elektronsko arhiviranje", Mat. Inst. SANU, Beograd, dec. 2003.

  [IV.9] M. Markovic, D. Bajic, M. Mihaljevic, D. Urosevic, Z. Markovic, D. Blagojevic, "Softver arhivskog centra za zasticeno elektronsko arhiviranje", Mat. Inst. SANU, Beograd, dec. 2003.

  [IV.10] M. Markovic, D. Bajic, M. Mihaljevic, D. Urosevic, Z. Markovic, D. Blagojevic, "Softver podsistema certifikacionog tela za zasticeno elektronsko arhiviranje", Mat. Inst. SANU, Beograd, dec. 2003.

  [IV.11] D. Urosevic, D. Bajic, M. Mihaljevic, M. Markovic, Z. Markovic, D. Blagojevic, "Improved-FEA-M - Softver II podsistema za zastitu tajnosti za zasticeno elektronsko arhiviranje: Implementacija novog algoritma za sifrovanje/desifrovanje", Mat. Inst. SANU, Beograd, dec. 2004.

  [IV.12] M. Markovic, D. Bajic, M. Mihaljevic, D. Urosevic, Z. Markovic, D. Blagojevic, "eEDocSecure - Softver sistema za zasticeno elektronsko arhiviranje, 1.10", Mat. Inst. SANU, Beograd, dec. 2004

  [IV.13] M. Markovic, D. Bajic, M. Mihaljevic, D. Urosevic, Z. Markovic, D. Blagojevic, "eEDocSecure-MISANU - Softver sistema za zasticeno elektronsko arhiviranje, 1.24", Mat. Inst. SANU, Beograd, dec. 2004