Začasna politika Certifikatne agencije @friCA

za digitalna potrdila za študente UL FRI in zaposlene

Verzija 1.0, 10. september 2007

1 Uvod

Ta dokument je *Začasna politika Certifikatne agencije @friCA Verzija 1.0 za digitalna potrdila za študente FRI, Univerza v Ljubljani, in zaposlene z dne 10. septembra 2007.* Organizacija, ki je odgovorna za vzdrževanje tega dokumenta, je

Univerza v Ljubljani Fakulteta za računalništvo in informatiko
Tržaška 25
1000 Ljubljana
Slovenija

(v nadaljevanju Certifikatna agencija @friCA). Certifikatna agencija @friCA je testna certifikatna agencija, ki deluje interno na Fakulteti za računalništvo in informatiko, Univerza v Ljubljani. Certifikatna agencija @friCA je korenska certifikatna agencija, ki izdaja digitalna potrdila in upravlja sezname preklicanih potrdil. Skrbi tudi za distribucijo in preklic potrdil preko temu namenjenega spletnega strežnika. Določa in objavlja svojo politiko delovanja ter skrbi za nemoteno delovanje svojih storitev v skladu s politiko. Politiko podpira obsežnejši dokument *Notranja pravila delovanja*, v katerem so podrobno opisani postopki, s katerimi Certifikatna agencija @friCA dosega zahteve iz politike.

Digitalna potrdila Certifikatne agencije @friCA, izdana po tej politiki, se uporabljajo za dostop do spletnih aplikacij, za katere se zahteva identifikacija s potrdili te certifikatne agencije, in za druge namene, za katere se med seboj dogovorijo uporabniki. Imetniki potrdil so študenti UL FRI, učitelji in sodelujoči pri upravljanju in razvoju certifikatne agencije.

Certifikatna agencija @friCA vzdržuje spletno stran, na kateri objavlja kontaktne podatke ter druge dokumente in imenike, glej razdelek 2. Za kontakte z uporabniki skrbi pooblaščena oseba iz Laboratorija za kriptografijo in računalniško varnost na UL FRI, katere elektronski naslov je objavljen na spletni strani Certifikatne agencije @friCA.

2 Objave informacij in imeniki potrdil

Certifikatna agencija @friCA v imenikih **hrani** naslednje podatke:

- evidenčne podatke o potrdilih (ime, priimek in za študente še vpisno številko),
- potrdila, ki jim še ni potekel rok veljavnosti,
- potrdila uporabnikov in zasebne ključe, ki jim še ni potekel rok veljavnosti do prevzema (v šifrirani obliki); vsako potrdilo posebej je zaščiteno z geslom,

- seznam preklicanih potrdil,
- politiko,
- notranja pravila delovanja (angl. Certificate Practice Statement),
- navodila za prevzem/naročilo/preklic in varno uporabo digitalnih potrdil.

Naslednji podatki v imenikih so dostopni samo pooblaščenim osebam: evidenčni podatki o potrdilih, potrdila, ki jim še ni potekel rok veljavnosti, zaupni del notranjih pravil delovanja. Imetniki potrdil lahko dostopajo do svojega potrdila z zasebnim ključem v imeniku potrdil; po prevzemu se le-ta izbriše iz seznama.

Certifikatna agencija @friCA vzdržuje spletno stran

`https://lkrv.fri.uni-lj.si/africa`,

ki je javno dostopna (dostop preko protokola `https`). Na tej spletni strani **objavlja** kontaktne podatke ter druge dokumente in imenike, kot so:

- politika,
- navodila za prevzem in varno uporabo digitalnih potrdil,
- obrazci z zahtevki za pridobitev ali preklic potrdil z navodili,
- kontaktni naslov (za sprejemanje zahtevkov za izdajo/preklic potrdil, informacije),
- potrdilo z javnim ključem Certifikatne agencije @friCA,
- seznam preklicanih potrdil.

Vsi dokumenti se na novo objavijo ob spremembi, seznam preklicanih potrdil pa se poleg tega objavlja redno, vsaj enkrat mesečno. O spremembah se imetnikov potrdil ne obvešča posebej, razen v primeru bistvenih sprememb politike, zaradi katerih bi se lahko spremenil nivo zaupanja.

3 Istovetnost imetnikov potrdil

Vsako potrdilo vsebuje podatke o imetniku ter izdajatelju v obliki razločevalnega imena, ki je oblikovano v skladu s standardom X.501. Podeljeno razločevalno ime je enolično za vsako potrdilo v uporabi. Razločevalno ime ne vsebuje osebnih podatkov (razen imena in priimka).

Ob sprejemu zahtevka se pred izdajo potrdila preveri upravičenost prosilca do potrdila. Istovetnost imetnika potrdila se preverja pri izdaji gesel za prevzem potrdila in ob preklicu potrdila. Pri preklicu potrdila preko spletnega obrazca, kjer je potrebno vnesti geslo za preklic, se istovetnosti ne preverja.

Preverjanje istovetnosti opravi pooblaščena oseba, ki preveri osebni dokument: študentska izkaznica ali indeks v primeru študenta, drug veljaven osebni dokument v primeru drugih oseb.

4 Upravljanje s potrdili

Potrdila se redno vpisanim študentom UL FRI izdajo avtomatično vsako leto ob vpisu. Za potrdila lahko zaprosijo študenti UL FRI, ki niso redno vpisani, in zaposleni na UL

FRI. Potrdila pridobijo tudi sodelavci/upravljalci Certifikatne agencije @friCA. Rok za izdajo potrdila je največ 14 dni od vložitve zahtevka. Navodila za pridobitev/prevzem/preklic potrdila so objavljena na spletni strani Certifikatne agencije @friCA.

Študentom prvega letnika (prvič vpisanim) se gesla za prevezem, zaščito in preklic potrdila razdeli ob podelitvi indeksov v začetku šolskega leta. Ostali prevzamejo gesla v študentski pisarni UL FRI. Imetniki prevzamejo potrdila s spletne strani preko protokola `https` in ga s pridobljenim geslom vključijo v svoj brskalnik.

Po tej politiki spreminjanje, obnova, podaljšanje in mirovanje potrdil niso podprti. V primeru, da obstajajo razlogi za spremembo/mirovanje potrdila, se potrdilo prekliče in izda novo.

Preklic potrdil

Preklic potrdila mora imetnik zahtevati v primeru:

- da obstaja nevarnost zlorabe zasebnega ključa ali potrdila imetnika,
- da je bil zasebni ključ imetnika potrdila izgubljen,
- da so se spremenili oz. so napačni ključni podatki, navedeni v potrdilu.

Certifikatna agencija @friCA lahko prekliče potrdilo tudi brez zahteve imetnika v naslednjih primerih, brž ko izve:

- da potrdilo ni bilo prevzeto v predpisanem roku,
- da je bilo potrdilo izdano na podlagi napačnih podatkov,
- da je prišlo do napake pri preverjanju istovetnosti podatkov pri izročitvi gesel in je potrdilo (morda) prevzela napačna oseba,
- da so se spremenile druge okoliščine, ki bistveno vplivajo na veljavnost potrdila,
- da je bil zasebni ključ imetnika potrdila ogrožen in nadaljna uporaba potrdila ne bi bila več varna,
- da je bila infrastruktura Certifikatne agencije @friCA ogrožena na način, ki vpliva na zanesljivost potrdila,
- da bo Certifikatna agencija @friCA prenehala z izdajanjem potrdil.

Preklic potrdila lahko zahteva imetnik potrdila ali pooblaščena oseba Certifikatne agencije @friCA. Imetnik potrdila ali certifikatna agencija sta dolžna zahtevati preklic takoj, ko nastopi eden od goraj omenjenih razlogov za preklic.

Postopek za preklic potrdila s strani imetnika potrdila je objavljen na spletni strani Certifikatne agencije @friCA in je sledeč. Imetnik lahko potrdilo prekliče preko spletnega obrazca, ki se nahaja na spletni strani agencije. V spletni obrazec vnese priimek, ime, serijsko številko potrdila, razlog za preklic in geslo za preklic potrdila, ki ga je prejel skupaj z geslom za prevzem potrdila. V primeru, da nima dostopa do gesla za preklic ali serijske številke, imetnik potrdilo prekliče osebno v študentski pisarni UL FRI. Certifikatna agencija @friCA podatke v zahtevku za preklic preveri ter ustrezna potrdila doda na seznam preklicanih potrdil in briše iz imenika veljavnih potrdil. V primeru, da preklic zahteva pooblaščena oseba Certifikatne agencije @friCA, se preveri ustreznost zahtevka in o preklicu obvesti imetnika.

Certifikatna agencija @afriCA se zavezuje, da bo postopek za preklic izvedla v roku največ 14 dni od vložitve zahtevka za preklic. Ob utemeljenem sumu, da je možna zloraba potrdila, potrdilo prekliče v roku enega dne.

Tretje osebe, ki se zanašajo na potrdilo, morajo pred uporabo preveriti najnovejši objavljeni seznam preklicanih potrdil, ki ga morajo osvežiti vsak dan. Pri tem morajo preveriti tudi verodostojnost tega seznama, ki je digitalno podpisan s strani Certifikatne agencije @friCA.

Če je ogrožen zasebni ključ Certifikatne agencije @friCA, se obvesti skrbnike aplikacij za dostop do varnih domačih strani, da ustrezno ukrepajo. Ob ugotovljeni realni možnosti za zlorabo se prekličejo vsa potrdila, ki jih je izdala certifikatna agencija @friCA, in izdajo nova.

5 Upravljanje in varnostni nadzor prostorov, opreme, postopkov in osebja

Fizično varovanje

Oprema Certifikatne agencije @friCA, na kateri se izvajajo kriptografske operacije, se nahaja v prostorih, do katerih lahko dostopajo samo pooblaščene osebe. Računalniška oprema je zaščitena pred električnim udarom in ima sistem za neprekinjeno napajanje, ki omogoča normalno delovanje vsaj eno uro od prekinitve oskrbe z električno energijo. Če po tem času ni vzpostavljeno delovanje električnega omrežja, se vse naprave samodejno izklopijo.

Nosilci varnostnih kopij so shranjeni v sefu, ki je odporen na vodo in ognjevaren. Nahajajo se v prostorih, ki so zaščiteni pred nepooblaščenim vstopom. Nosilci podatkov se pred odstranitvijo varno uničijo tako, da ni več mogoče rekonstruirati njihove vsebine. Varnostne kopije zasebnega ključa Certifikatne agencije @friCA in podatkov za delovanje certifikatne agencije se hranijo na vsaj dveh različnih lokacijah.

Organizacijska struktura overitelja in nadzor osebja

Vse postopke v zvezi z delovanjem Certifikatne agencije @friCA vodi Laboratorij za kriptografijo in računalniško varnost na UL FRI. Pri sprejemanju zahtevkov za izdajo/preklic potrdil in distribuciji gesel za prevzem potrdil sodeluje študentska pisarna UL FRI. Dostop do zasebnega ključa Certifikatne agencije @friCA za izdajo potrdil in seznamov preklicanih potrdil imajo vsaj tri pooblaščene strokovno usposobljene osebe. Interni nadzor osebja izvaja vodja Laboratorija za kriptografijo in računalniško varnost, zunanji nadzor pa izvaja komisija, sestavljena iz strokovnih sodelavcev na UL FRI.

Varnostni pregledi sistema

Upravljalci Certifikatne agencije @friCA so dolžni voditi dnevnike, v katere se zapisujejo vse dejavnosti v zvezi s postopki agencije. Dnevniki se redno pregledujejo in varno hranijo. Podrobneje je vodenje dnevnikov določeno v *Zaupnem delu notranjih pravil delovanja Certifikatne agencije @friCA*.

Arhiviranje podatkov

Certifikatna agencija @friCA arhivira podatke v skladu z zakonom ZEPEP, kar je podrobno

določeno v *Zaupnem delu notranjih pravil delovanja Certifikatne agencije @friCA*.

Okrevalni načrt

Certifikatna agencija @friCA ima v *Zaupnem delu notranjih pravil delovanja* sestavljen podroben načrt za naslednje postopke:

- postopek v primeru vdorov in zlorabe,
- postopek v primeru okvare strojne opreme, programske opreme ali podatkov,
- postopek v primeru ogroženega zasebnega ključa Certifikatne agencije @friCA,
- nadaljevanje dejavnosti po morebitni katastrofi.

Prenehanje delovanja Certifikatne agencije @friCA

Potrdila uporabnikov Certifikatne agencije @friCA imajo razmeroma kratek rok veljavnosti, zato je predvideno, da lahko @friCA preneha z delovanjem po preteku veljavnosti vseh izdanih potrdil uporabnikov. V primeru, da bi Certifikatna agencija @friCA prenehala z delovanjem prej, prekliče vsa potrdila, ki so v tem času še veljavna, in vzdržuje seznam preklicanih certifikatov do preteka veljavnosti vseh izdanih potrdil. Ta seznam ima daljši rok veljavnosti in se ne obnavlja.

6 Tehnične varnostne zahteve

Generiranje para ključev in namestitev

Vse ključe, vključno s ključi za korensko potrdilo Certifikatne agencije @friCA, generira Certifikatna agencija @friCA sama. Generirajo se s programsko opremo Certifikatne agencije @friCA, ki upošteva zahteve standarda IEEE P1363. S tem je zagotovljena primerna kvaliteta ključev.

Dolžina ključev je glede varnosti enakovredna: za imetnike potrdil ključem za RSA dolžine vsaj 1024 bitov, za strežnike vsaj 2048 bitov in za korensko potrdilo Certifikatne agencije @friCA vsaj 2048 bitov.

Zaščita zasebnega ključa

Zasebni ključ Certifikatne agencije @friCA se nahaja v kriptografskem modulu, kjer je dostopen le pooblaščenim osebam. Ob generiranju se ustvarita vsaj dve varnostni kopiji, ki se varno hranita na različnih lokacijah.

Zasebne ključe ostalih uporabnikov se iz kriptografskega modula ob generiranju prenese na spletni strežnik s pomočjo prenosnega pomnilnega medija, kjer se do prevzema hranijo v šifrirani obliki, zaščiteni z geslom.

Ostali vidiki upravljanja ključev

Obdobje veljavnosti za potrdilo in ustrezne pare ključev je enako. Potrdila imetnikom se izdajajo za obdobje enega šolskega leta, podaljšanega za en mesec, torej največ za 14 mesecev (od 1. septembra do 31. oktobra naslednjega leta). Korensko potrdilo Certifikatne agencije

@friCA je izdano za obdobje 10 let.

Naslednja gesla generira Certifikatna agencija @friCA naključno: geslo za prevzem potrdila, geslo za zaščito zasebnega ključa imetnika in geslo za preklic potrdila. Vsa gesla morajo biti dolga vsaj 15 znakov (alfanumerični znaki in nekateri znaki, ki so enostavno dostopni preko standardnih tipkovnic).

Varnostne zahteve za računalniško opremo overitelja

Računalnik Certifikatne agencije @friCA, na katerem se generirajo ključi in potrdila, ni priključen na nobeno računalniško omrežje. Dostop je nadzorovan in omogočen le pooblaščenim osebam za dela v zvezi s tekočim vzdrževanjem in opravljanjem nalog agencije. Vsi podatki na računalniku se hranijo v šifrirani obliki. Prenos podatkov iz računalnika je možen le s prenosnim medijem.

Spletni strežnik, na katerem se nahajajo imeniki, mora biti zaščiten s požarnim zidom, ki dovoljuje prehod samo protokolom, ki so nujni za delovanje. Dostopi do strežnika se kontrolirajo s sistemom za odkrivanje in preprečevanje vdorov IDS/IPS (intrusion detection system/intrusion prevention system). Uporabniška imena, zaščitena z geslom, imajo na strežniku le pooblaščene osebe, ki upravljajo z imeniki in spletnimi aplikacijami. Računalnik se uporablja le za administriranje imenikov in vzdrževanje aplikacij.

Tehnični nadzor razvoja overitelja

Primernost varnostnih nastavitev, opisanih v tej politiki in v *Notranjih pravilih delovanja*, se preveri vsako leto. Oceni se varnostno tveganje in na osnovi tega odloči, ali je potrebno dopolniti postopke Certifikatne agencije @friCA in/ali povečati predpisane dolžine ključev, da se ohrani varnost sistema.

7 Profil potrdil in seznama preklicanih potrdil

Vsa potrdila Certifikatne agencije @friCA sledijo standardu X.509, različici 3, in so digitalno podpisana z zasebnim ključem Certifikatne agencije @friCA. Vsako potrdilo vsebuje podatke o imetniku ter izdajatelju v obliki razločevalnega imena, ki je oblikovano v skladu s standardom X.501. Podeljeno razločevalno ime je enolično za vsako potrdilo v uporabi in ne vsebuje osebnih podatkov. Vsako potrdilo vsebuje tudi javni ključ, ki je glede varnosti ekvivalenten vsaj ključem za RSA dolžine 1024 bitov.

Seznami preklicanih potrdil sledijo standardu X.509, verziji 2 za sezname preklicanih potrdil, in so digitalno podpisani z zasebnim ključem Certifikatne agencije @friCA. Ob preklicu se v seznam preklicanih potrdil za vsako preklicano potrdilo doda njegovo enolično serijsko številko ter čas in datum preklica.

8 Inšpekcijski nadzor

Ni predvideno.

9 Finančne in ostale pravne zadeve

Ceniki

Upravljanje z digitalnimi potrdili Certifikatne agencije @friCA je za uporabnike potrdil brezplačno.

Finančna odgovornost

UL Fakulteta za računalništvo in informatiko - Certifikatna agencija @friCA ne nosi nobene finančne odgovornosti za škodo, ki bi nastala ob nepravilni in tudi ob pravilni uporabi njenih potrdil.

Varovanje podatkov

Certifikatna agencija @friCA ravna zaupno z vsemi osebnimi podatki, s katerimi razpolaga, in jih ne posreduje tretjim osebam. Osebni podatki so varovani v skladu z zakonom o varstvu osebnih podatkov.

Določbe glede avtorskih, sorodnih in drugih pravic intelektualne lastnine

Certifikatni agenciji @friCA pripadajo vse pravice na pričujoči politiki. Na imeniku potrdil, seznamu preklicanih potrdil in na vseh podatkih v potrdilih pripadajo vse pravice Certifikatni agenciji @friCA.

Obveznosti in odgovornosti

Obveznosti in odgovornosti @friCA. Certifikatna agencija @friCA je dolžna delovati v skladu s svojo politiko in izdajati digitalna potrdila upravičencem, na zahtevo preklicati potrdila in izdajati sezname preklicanih potrdil v zato določenih rokih. Certifikatna agencija @friCA je odgovorna za izvajanje vseh določil iz te politike.

Obveznost in odgovornost prijavne službe. Ob izdaji gesel za prevzem potrdila in ob preklicu potrdila (če ni elektronsko) pooblaščena oseba v prijavni službi (študentski referat UL FRI) preveri osebni dokument. Preveri upravičenost sprejetih zahtevkov in jih posreduje naprej v obdelavo pooblaščenim osebam Certifikatne agencije @friCA v roku največ enega tedna, v primeru preklica potrdila z možnostjo zlorabe pa še isti dan. Prijavna služba je odgovorna za izvajanje zgoraj naštetih določil.

Obveznosti in odgovornost imetnika potrdila. Imetnik oziroma bodoči imetnik potrdila je dolžan:

- podatke za prevzem potrdila skrbno varovati pred nepooblaščenimi osebami,
- po prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah zahtevati preklic potrdila,
- varno hraniti zasebni ključ in ga ščititi s primernim geslom,
- skrbno varovati geslo za zaščito zasebnega ključa,
- zahtevati preklic potrdila, če je bil zasebni ključ ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe,
- seznaniti se in ravnati v skladu s politiko Certifikatne agencije @friCA,

- uporabljati potrdilo samo za namen, ki je določen s politiko.

Imetnik odgovarja za škodo, ki bi nastala zaradi nepravilne uporabe potrdila, ter za škodo v primeru zlorabe potrdila od časa prejema zahtevka za preklic do samega preklica potrdila.

Obveznosti in odgovornost tretjih oseb. Tretje osebe, ki se zanašajo na potrdilo, morajo pred uporabo preveriti veljavnost potrdila in najnovejši objavljeni seznam preklicanih potrdil. Na potrdila se lahko zanašajo le za namen, za katerega je potrdilo izdano. Tretje osebe odgovarjajo za škodo, ki bi nastala zaradi neupoštevanja zgoraj naštetih določil.

Veljavnost politike

Politika je veljavna do preklica ali objave nove politike, vendar največ toliko časa, kolikor obstaja Certifikatna agencija @friCA.

Ob izdaji nove politike se vsa potrdila izdana po tem datumu obravnavajo po novi politiki. Potrdila izdana po prejšnjih politikah ostanejo v veljavi do konca preteka veljavnosti in se obravnavajo po novi politiki, kjer je to možno. V veljavi ostanejo tista določila stare politike, ki se smiselno ne morejo nadomestiti z ustreznimi določili nove politike.

Veljavna zakonodaja

V Sloveniji je osnova za poslovanje z digitalnimi potrdili *Zakon o elektronskem poslovanju in elektronskem podpisu ZEPEP* [3] in na njegovi osnovi izdana *Uredba o elektronskem poslovanju in elektronskem podpisovanju* [4].

Certifikatna agencija @friCA je agencija zaprtega tipa, zato določbe zakona ZEPEP, z izjemo določb 4. in 14. člena, zanjo ne veljajo. Politika se ravna po zakonu čim bolj, tam kjer je to smiselno.

Literatura

[1] S. Chokhani, W. Ford, R. Sabett, C. Merrill in S. Wu: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, 2003, `http://ietf.org/rfc/rfc3647.txt`

[2] ETSI TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, `http://www.etsi.org/`

[3] Zakon o elektronskem poslovanju in elektronskem podpisu /ZEPEP/ Ur.l. RS, 57/2000 in 30/2001; uradno prečiščeno besedilo je v Ur. l. RS 98/2004.

[4] Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje Ur. l. RS 77/2000 in 2/2001.

[5] Politika SIGEN-CA za kvalificirana digitalna potrdila za fizične osebe, Javni del notranjih pravil overitelja na Ministrstvu za javno upravo, verzija 3.1., 18. maj 2007.