



(19) REPUBLIKA HRVATSKA
DRŽAVNI ZAVOD ZA
INTELEKTUALNO VLASNIŠTVO

(10) Identifikator
dokumenta:



HR P20160140 T1

HR P20160140 T1

(12) **PRIJEVOD PATENTNIH ZAHTEJEVA
EUROPSKOG PATENTA**

(51) MKP:

H04L 29/06 (2006.01)

(46) Datum objave prijevoda patentnih zahtjeva: 25.03.2016.

(21) Broj predmeta: P20160140T

(22) Datum podnošenja zahtjeva: 08.02.2016.

(96) Broj europske prijave patenta: EP 12188046.2
Datum podnošenja europske prijave patenta: 10.10.2012.

(97) Broj objave europske prijave patenta: EP 2582115 A1
Datum objave europske prijave patenta: 17.04.2013.

(97) Broj objave europskog patenta: EP 2582115 B1
Datum objave europskog patenta: 09.12.2015.

(31) Broj prve prijave: TO20110902 (32) Datum podnošenja prve prijave: 10.10.2011. (33) Država ili organizacija podnošenja prve prijave: IT

(73)(72) Nositelj patenta i izumitelj: **Antonio Salvatore Piero Vittorio Bonsignore, Via Paisiello 21, 20011 Corbetta, MI, IT**

(74) Zastupnik: **Odvjetničko društvo Vukmir i suradnici, 10000 Zagreb, HR**

(54) Naziv izuma: **KVALIFICIRANI ELEKTRONSKI SUSTAV ZA POTPISIVANJE, ODGOVARAJUĆI POSTUPAK I UREĐAJ MOBILNOG TELEFONA ZA KVALIFICIRANI ELEKTRONSKI POTPIS**

HR P20160140 T1

PATENTNI ZAHTJEVI

- 5
1. Kvalificirani sustav elektronskog potpisa koji je konfiguriran za izmjenjivanje podataka s prvim sredstvima za obradu (100; 303; 210) podnositelja zahtjeva (300; 400) konfiguriranim da omogućavaju navedenom podnositelju zahtjeva (300, 400) da kroz navedeni sustav generira navedene sistemske zahtjeve (305) vezane za potpisnika (365; 400), te navedeni sustav sadrži druga sredstva za obradu (210) potpisnika (365; 400) konfigurirana da omogućuje navedenom potpisniku (365; 400) potpisivanje s njegovim kvalificiranim elektronskim potpisom, navedena druga sredstva za obradu (210) koja sadrže uređaj mobilnog telefona za omogućavanje navedenom potpisniku potpisivanje s njegovim kvalificiranim elektronskim potpisom mobilnog tipa, prilagođena za prijem (340) i slanje (345) tekstualnih poruka na mobilnim telekomunikacijskim mrežama koje sadrže jedan ili više poslužitelja, ili za prijem (351) i slanje (352) elektronskih podataka s modulima za blizinu na bliskim mrežama, na temelju identifikatora navedenog potpisnika kao pretplatnika mobilne telefonske usluge navedeni identifikator je sadržan u modulu identiteta pretplatnika (SIM) (120) s kojim je povezan navedeni potpisnik, pri čemu: navedena druga sredstva za obradu (210) sadrže sredstva (220) za provođenje navedenog kvalificiranog elektronskog potpisa putem sigurnosne memorije (200) koja sadrži barem sigurnu particiju u kojoj je pohranjen barem privatni ključ (201) navedenog potpisnika, navedeni elektronski potpis se provodi u navedenoj sigurnoj particiji navedene sigurnosne memorije certificiranoj za kvalificirani elektronski potpis i za pohranjivanje navedenog privatnog ključa na neovisan način s obzirom na navedenu mobilnu telefonsku uslugu, na navedenim mobilnim telekomunikacijskim mrežama i do navedenog modula identiteta pretplatnika (SIM) (120), te se navedena sigurnosna memorija (200) aktivira kako bi mogla provoditi kvalificirani elektronski potpis na temelju aktivacijskog koda koji je unesen od strane navedenog potpisnika putem spomenutog uređaja mobilnog telefona; navedena sigurnosna memorija je različita od navedenog modula identiteta pretplatnika (SIM) i moguće joj je pristupiti putem spomenutog uređaja mobilnog telefona u kombinaciji s navedenim modulom identiteta pretplatnika (SIM) kao identifikatorom navedenog potpisnika s kojim je povezana navedena sigurnosna memorija, kada se podaci izmjenjuju putem navedenih mobilnih telekomunikacijskih mreža, ili u kombinaciji navedenih elektronskih podataka (351, 352) kada se podaci izmjenjuju kroz navedene bliske mreže, navedeni sustav kvalificiranog elektronskog potpisa također sadrži namjensku poslužiteljsku mrežu (302, 310, 315), različitu od navedenih poslužitelja navedenih mobilnih telekomunikacijskih mreža, radi provođenja komunikacije između navedenih prvih sredstava za obradu (100; 303; 210) podnositelja zahtjeva i navedenih drugih sredstava za obradu (210) potpisnika; navedena namjenska poslužiteljska mreža obuhvaća barem:
- jedan front-end poslužitelj (310) konfiguriran za primanje, provjeru i otpremanje navedenih sistemskih zahtjeva (305), koji zahtijevaju navedeni kvalificirani elektronski potpis ili koji sadrže navedeni kvalificirani elektronski potpis, radi generiranja otpremljenih zahtjeva (308), te se navedeni sistemski zahtjevi (305) šalju pomoću navedenih prvih sredstava za obradu (100; 303; 210) jedan ili više aplikacijskih poslužitelja (315) konfiguriranih za primanje i provjeru navedenih otpremljenih zahtjeva (308), te kada se podaci izmjenjuju putem navedenih mobilnih telekomunikacijskih mreža, konfiguriran da također šalje navedene tekstualne komunikacije (340) na spomenute mobilne telekomunikacijske mreže;
 - navedeni front-end poslužitelj (310) je konfiguriran za slanje navedenih otpremljenih zahtjeva (308) na odgovarajući aplikacijski poslužitelj (315) na temelju identifikatora potpisnika (365; 400) ili njegovog broja telefona, koji se povezan s navedenim modulom identiteta pretplatnika (SIM), te na temelju vrste zahtjeva (305);
 - navedeni aplikacijski poslužitelj (315) je konfiguriran da proslijeđuje navedeni zahtjev (305) kao tekstualnu komunikaciju (340) na mobilnu telekomunikacijsku mrežu pomoću navedenog identifikatora pretplatnika mobilne telefonske usluge u navedenom modulu identiteta pretplatnika (SIM) (120) do navedenih drugih sredstava za obradu (210), kada se podaci izmjenjuju putem navedenih mobilnih telekomunikacijskih mreža;
 - navedena druga sredstva za obradu (210) su također konfigurirana da (220):
 - koriste navedeni privatni ključ (201) u navedenoj sigurnosnoj memoriji (200) i da potpisuju s navedenim kvalificiranim elektronskim potpisom pomoću enkripcije sažetka navedene tekstualne komunikacije na mobilnoj telefonskoj mreži (340), ili pomoću enkripcije sažetka navedenih elektronskih podataka (351) primljenih putem navedenih bliskih mreža, ili njihovih dijelova pomoću navedenog privatnog ključa (201);
 - šalju navedeni potpis do aplikacijskog poslužitelja (315) putem potvrdne poruke (345), kada se podaci izmjenjuju putem navedenih mobilnih telekomunikacijskih mreža, ili šalju poruku (352) do navedenih prvih sredstava podnositelja zahtjeva, kada se podaci izmjenjuju putem navedenih bliskih mreža.
2. Sustav prema zahtjevu 1, **naznačen time** da je navedena potvrdna poruka (345) u obliku SMS (Short Message System) tekstualnih poruka, ili je obliku elektronskih podataka (352) koji su pogodni za izmjenjivanje s bliskim mrežama, te se navedeni otpremljeni zahtjev (308) proslijeđuje kao tekstualna komunikacija (340) na mobilnu telekomunikacijsku mrežu u obliku tekstualne poruke SMS tipa.

3. Sustav prema zahtjevu 1 ili 2, **naznačen time** da navedeni zahtjev (305) je zahtjev za plaćanje ili zahtjev za pretplatu na dokument ili pristup ili zahtjev za narudžbu mrežnih usluga, te navedeni zahtjev (305) sadrži navedeni identifikator navedenog potpisnika.
4. Sustav prema jednom ili više od prethodnih zahtjeva, **naznačen time** da je navedeni front-end poslužitelj (310) konfiguriran, u navedenom postupku validacije, da dodaje varijabilni dio koji sadrži barem jedan jedinstveni identifikator i vremensku oznaku zahtjeva (305) ili za validaciju navedenog promjenjivog dijela i navedene vremenske oznake ako je primljena u navedenom zahtjevu (305).
5. Sustav prema jednom ili više od prethodnih zahtjeva, **naznačen time** da je uređaj mobilnog telefona (210) konfiguriran da automatski prikazuje na zaslonu (110) tekstualni zahtjev (340) koji je primljen i da šalje, nakon potpisivanja s navedenim elektronskim potpisom, samostalni kvalificirani elektronski potpis, na aplikacijski poslužitelj (315) radi omogućavanja ovlaštene identifikacije potpisnika pomoću certifikata koji se nalazi u aplikacijskom poslužitelju (315) na temelju certifikata tijela za izdavanje certifikata koje ga je izdalo, oba certifikata su povezani s navedenim potpisnikom, ili je navedeni uređaj mobilnog telefona (210) također konfiguriran da automatski prikazuje na zaslonu (110) zaprimljeni zahtjev (351), te da šalje, nakon potpisivanja s navedenim elektronskim potpisom, samostalni kvalificirani elektronski potpis (352) do navedenih prvih sredstava podnositelja zahtjeva radi omogućavanja ovlaštene identifikacije potpisnika pomoću certifikata u aplikacijskom poslužitelju (315) na temelju certifikata tijela za izdavanje certifikata koje ga je izdalo, te su oba certifikata povezana s navedenim potpisanim korisnikom (365; 400).
6. Sustav prema jednom ili više od prethodnih zahtjeva, **naznačen time** da navedeni barem jedan front-end poslužitelj (310) sadrži bazu podataka registriranih korisnika namjenske poslužiteljske mreže (302, 310, 315), te je konfiguriran da provjerava u navedenoj bazi podataka registriranih korisnika, prisutnost potpisnika (365; 400) i informaciju povezanu s navedenim potpisnikom (365; 400), radi usmjeravanja zahtjeva (305) prema navedenom odgovarajućem aplikacijskom poslužitelju (315) potpisnika (365; 400).
7. Sustav prema zahtjevu 5 ili 6, **naznačen time** da je navedeni aplikacijski poslužitelj (315) konfiguriran za provjeru navedenog kvalificiranog elektronskog potpisa koji šalje uređaj mobilnog telefona (210) i za aktiviranje instrukcija za transakciju koje se određuju na temelju vrste zahtjeva (305).
8. Sustav prema jednom ili više zahtjeva od 5 do 7, **naznačen time** da je navedeni aplikacijski poslužitelj (315) na temelju jedinstvenog identifikatora radnog zahtjeva (305) konfiguriran za obnavljanje odgovarajućeg statusa rada na front-end poslužitelju (310).
9. Sustav prema jednom ili više od prethodnih zahtjeva, **naznačen time** da su navedena prva sredstva za obradu podnositelja zahtjeva također konfigurirana kao navedena druga sredstva za obradu (210), te sadrže uređaj mobilnog telefona, pogodan za izmjenjivanje tekstualnih komunikacija na mobilnim telekomunikacijskim mrežama, ili za izmjenjivanje elektronskih podataka s modulima blizine na bliskim mrežama, na temelju identifikatora pretplatnika mobilne telefonske usluge koji su sadržani u modulu identiteta pretplatnika (SIM) (120) sa kojim je povezan i sredstvima (220) za upravljanje sa sigurnosnom memorijom koja sadrži sigurnu particiju u kojoj je pohranjen privatni ključ (201).
10. Sustav prema jednom ili više od prethodnih zahtjeva, **naznačen time** da navedena prva sredstva za obradu (100; 303; 210) podnositelja zahtjeva odgovaraju navedenim drugim sredstvima za obradu (210) potpisnika.
11. Sustav prema jednom ili više od prethodnih zahtjeva, **naznačen time** da sadrži računalo predviđeno s sredstvima za prikaz koja su veća od sredstava za prikaz spomenutog uređaja mobilnog telefona i **time da** se navedeni otpremljeni zahtjev (308) također šalje kao e-mail poruka na adresu koja može biti dostupna navedenom potpisniku, te navedena e-mail poruka sadrži informacije, naročito adresnu referencu, za predočavanje jednog ili više dokumenata povezanih s navedenim otpremljenim zahtjevom (308), naročito dokumente na koje se pretplaćuje, na navedenim većim sredstvima za prikazivanje.
12. Sustav prema jednom ili više od prethodnih zahtjeva, **naznačen time** da se navedena potvrdna poruka (345) ili tekstualna poruka (340) ili obje navedene poruke odgovarajuće prenose i primaju u obliku bežične komunikacije putem bežičnog spojnog modula (121), te naročito kao e-mail poruka ili *push* poruka ili druga komunikacija koja se prenosi na Internet.
13. Sustav prema jednom ili više od prethodnih zahtjeva, **naznačen time** da koristi certifikate izdane od strane tijela koja izdaju certifikate povezane s navedenom namjenskom poslužiteljskom mrežom (302, 310, 315) za proceduru elektronskog potpisa koja je ekvivalentna kvalificiranom elektronskom potpisu ili općenito proceduri elektronskog potpisa.
14. Sustav prema jednom ili više od prethodnih zahtjeva, **naznačen time** da navedena druga sredstva za obradu (210) sadrže jedno ili više sredstava za pohranjivanje za navedeni privatni ključ, te su navedena sredstva za pohranjivanje različita od navedene sigurnosne memorije (200), te naročito, ugrađena u, ili povezana s navedenim drugim sredstvima za obradu (210) potpisnika ili ugrađena u modul identiteta pretplatnika (SIM) (120), certificiran ili ne certificiran za kvalificirani elektronski potpis, te navedena sredstva (220) provode postupak navedenog elektronskog potpisa kojeg su mogućnosti pronaći i koriste najsigurnija sredstva za pohranjivanje među navedenim sredstvima za pohranjivanje na temelju unaprijed utvrđenog jamstvenog kriterija radi sprečavanja ekstrakcije privatnog ključa i/ili za izvršavanje RSA algoritma na siguran način.

15. Postupak kvalificiranog elektronskog potpisa **naznačen time** da sadrži operacije koje se primjenjuju od strane sustava za kvalificirani elektronski potpis prema jednom ili više zahtjeva od 1 do 14.
16. Postupak kvalificiranog elektronskog potpisa prema zahtjevu 15 **naznačen time** da sadrži: u zahtjevu (305) koji se unosi u prva sredstva za obradu (303; 100; 210) sadrži također privremenu zaporku (ATP); prikazivanje nesažetog osnovnog niza ili sažimanje navedenog osnovnog niza i navedene privremene zaporke na drugim sredstvima za obradu potpisnika (400); prikazivanje navedenog nesažetog osnovnog niza ili sažimanje navedenog osnovnog niza i navedene privremene zaporke na prvim sredstvima za obradu (303; 100; 210) podnositelja zahtjeva, navedeni postupak naročito sadrži izračunavanje od strane navedenog aplikacijskog poslužitelja (315) navedenog nesažetog osnovnog niza ili navedenog sažimanja navedenog osnovnog niza na temelju informacije o zahtjevu (305) i o navedenoj privremenoj zaporki (ATP), te o dodatnoj informaciji koja sadrži identifikator prijave na poslužitelju sučelja (302) koja odgovara identifikatoru zahtjeva (305).
17. Uređaj mobilnog telefona za kvalificirani elektronski potpis, prilagođen za izmjenjivanje tekstualnih komunikacija na mobilnim telekomunikacijskim mrežama, ili za izmjenjivanje elektronskih podataka s modulima za blizinu na bliskim mrežama, na temelju identifikatora pretplatnika mobilne telefonske usluge koji je sadržan u modulu identiteta pretplatnika (SIM) (120) s kojim je povezan navedeni pretplatnik, koji sadrži operativni sustav i sredstva (220) za rad sa sigurnosnom memorijom koja sadrži barem sigurnu particiju u kojoj je pohranjen barem privatni ključ (201) navedenog pretplatnika, te je navedena sigurnosna memorija različita od navedenog modula identiteta pretplatnika (SIM) i može joj se pristupiti s navedenim uređajem mobilnog telefona samo u suradnji s navedenim modulom identiteta pretplatnika (SIM) koji identificira navedenog potpisnika s kojim je povezana navedena sigurnosna memorija, te je navedeni uređaj mobilnog telefona konfiguriran, kroz namjensku softversku aplikaciju koja se izvršava u navedenom operativnom sustavu, da koristi navedeni privatni ključ (201) u navedenoj sigurnosnoj memoriji (200) i da potpisuje s kvalificiranim elektronskim potpisom pomoću enkripcije zatražene poruke (340) ili podataka (351) ili njihovih dijelova pomoću navedenog privatnog ključa (201), navedeni uređaj mobilnog telefona je u mogućnosti obraditi navedeni elektronski potpis u navedenoj sigurnoj particiji navedene sigurnosne memorije čuvanjem navedenog privatnog ključa na neovisan način s obzirom na navedenu mobilnu telefonsku uslugu, do navedenih mobilnih telekomunikacijskih mreža i do navedenog modula identiteta pretplatnika (SIM) (120) na temelju aktivacijskog koda unesenog od strane navedenog potpisnika putem spomenutog uređaja mobilnog telefona.