

(19)



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSKI RAZVOJ IN TEHNOLOGIJO
URAD RS ZA INTELEKTUALNO LASTNINO

(10)

SI 25003 A

(12)

PATENT(21) Številka prijave: **201600122**

(51) Int. Cl. (2016.01)

(22) Datum prijave: **04.05.2016****G06F 21/00****G06F 3/00**(45) Datum objave: **30.11.2016**

(30) Prednostna pravica:

04.05.2015 CZ PUV 2015-31036

(72) Izumitelji: **Jan Bednar, 377 01 Jindrichuv Hradec III, CZ;**
Ivan Janoušek, 277 15 Tišice, CZ;
Šimon Kubišta, 130 00 Praha 3, CZ

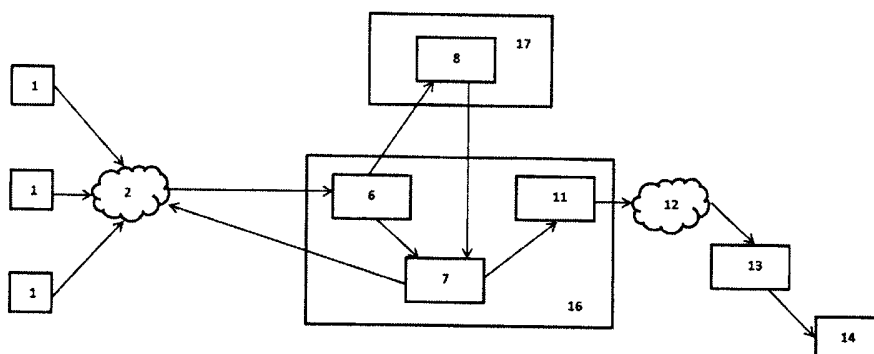
(73) Imetniki: **Jan Bednar,**
Rečička 795, 377 01 Jindrichuv Hradec III, CZ;
Ivan Janoušek,
Mezi Ploty 309, 277 15 Tišice, CZ;
Šimon Kubišta,
Vinohradska 168, 130 00 Praha 3, CZ

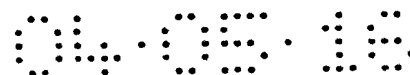
(74) Zastopnik: **PETOŠEVIČ d.o.o., Cankarjeva cesta 4, 1000 Ljubljana, SI**

(54) SISTEM ZA CERTIFICIRANJE ELEKTRONSKE POŠTE

(57) Sistem za certificiranje elektronske pošte obsega terminalno napravo (1) pošiljatelja elektronske pošte, ki jo je mogoče medsebojno povezati s strežnikom za odhodno elektronsko pošto (16), ki ga je mogoče povezati s strežnikom za dohodno elektronsko pošto (13), na katerega je nato mogoče povezati terminalno napravo

(14) prejemnika elektronske pošte. Strežnik za odhodno elektronsko pošto (16) je mogoče medsebojno povezati s strežnikom (17) kvalificiranega organa za certificiranje, pri čemer strežnik (17) kvalificiranega organa za certificiranje obsega notranji generator časa (8).

**SI 25003 A**



Sistem za certificiranje elektronske pošte

Področje tehnike, na katerega se izum nanaša

Izum se nanaša na sistem za certificiranje elektronske pošte (e-pošta), ki obsega terminalno napravo pošiljatelja e-pošte, ki jo je mogoče medsebojno povezati s strežnikom za odhodno e-pošto, ki ga je mogoče povezati s strežnikom za dohodno e-pošto, na katerega je nato mogoče povezati terminalno napravo prejemnika e-pošte.

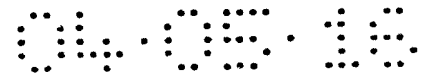
Stanje tehnike

Trenutno stanje elektronske komunikacije v glavnem temelji na izvirnih načelih internetnega povezovanja, ki poudarja visoko variabilnost možnih komunikacijskih sredstev, vendar pa na osnovni ravni ni opredeljeno za komunikacijo, ki bi zahtevalo visoko stopnjo verodostojnosti ali ki bi sploh ponujalo možnost preverjanja tovrstne komunikacije s strani enega izmed javnih organov oblasti.

Znani sistemi za elektronsko komunikacijo obsegajo terminalno napravo pošiljatelja e-pošte, ki jo je mogoče medsebojno povezati s strežnikom za odhodno e-pošto, ki ga je mogoče povezati s strežnikom za dohodno e-pošto, na katerega je nato mogoče povezati terminalno napravo prejemnika e-pošte.

Strežnik za odhodno e-pošto uporablja protokol „Simple Mail Transfer Protocol“ (kratica SMTP), strežnik za dohodno e-pošto pa za dostop prejemnika do sporočila uporablja protokol POP3 ali IMAP. Operater e-poštnih storitev deluje s sporočilom izključno na ravni odhodne ali dohodne elektronske pošte, ki je nameščena zgolj na osnovi splošnih standardov brez poudarka na veljavnosti informacij o izvedeni elektronski komunikaciji.

Informacije o vsebini elektronske pošte, o času in statusu prenosa se obdelujejo in shranjujejo zgolj na ravni lokalne naprave pošiljatelja in prejemnika e-poštnega



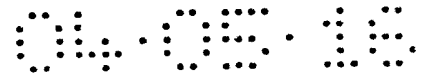
sporočila. Dnevnik operaterja e-poštnih storitev v večini primerov ni sledljiv, njegova veljavnost pa je lahko vedno vprašljiva.

V trenutni skupnosti, v kateri živimo, se pomen elektronskega komuniciranja povečuje, saj prihaja do premika od konvencionalne „papirnat“ pogodbene dokumentacije za izvedbo številnih pravnih korakov do standardne elektronske pošte.

Vendar pa trenutna elektronska pošta ne predvideva možnosti nespornega preverjanja vsebine ali časa pošiljanja. Dvomi glede vsebine in časa pošiljanja e-pošte imajo nato glavni vpliv na pogajanja strank in hkrati na pravno varnost udeležencev v pogajanjih.

Sistem, ki je trenutno na razpolago za potrjeno dostavo e-poštnih sporočil je, npr. informacijski sistem podatkovnih strani, ki jih upravlja podjetje Česká pošta s.p. (Češka pošta), vendar pa se ta storitev upravlja popolnoma ločeno od sredstev standardne e-poštne komunikacije, izvaja se v okviru posebnih uporabniških vmesnikov in njen odstotek zastopanosti v skupni komunikaciji je na precej nizki oziroma manjšinski ravni. Ne omogoča uporabe standardne komunikacije e-poštnih odjemalcev, ne le z vidika generacijskih orodij tovrstne komunikacije, temveč tudi z vidika uveljavljenih datotečnih storitev za delo z dokumenti. Udobje sistema podatkovnih strani je zelo nizko v primerjavi z udobjem konvencionalne e-poštne komunikacije.

Stanje tehnike nadalje omogoča uporabo storitve časovnega žiga (opredeljeno z Zakonom št. 227/2000 Coll., o elektronskem podpisu), da natančno ujame trenutek nastanka in vsebine datoteke, shranjene na lokalni ravni, npr. v uporabnikovem računalniku. Vendar pa čas pošiljanja e-poštnega sporočila, ki je potrjen na ta način, ni dokončen, saj ta postopek ujame trenutek nastanka e-poštnega sporočila, vendar zgolj na podlagi informacije, ki je uporabljena s strani uporabnikove lokalne postaje, tj. temelji na prilagodljivem sistemu časovnih nastavitev uporabnikove postaje. Obenem pošiljanja tudi ni mogoče preveriti, saj lahko pride do ugovora, da tako



sporočilo ni bilo izročeno za pošiljanje, npr. zaradi napake v internetni povezavi ali napake na strežniku ponudnika elektronskih komunikacijskih storitev, zaradi česar sporočilo ni bilo dostavljeno prejemniku, teh ugovorov pa v trenutnem stanju tehnike ni mogoče ovreči.

Namen izuma je predlagati takšen sistem, ki bo omogočal certificiranje elektronske pošte, ki se pogosto uporablja. Za potrebe te prijave se certificiranje nanaša na objektivno preverjanje vsebine in časa pošiljanja elektronske pošte.

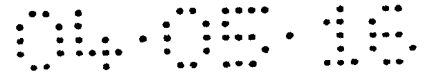
Opis izuma

Zgoraj navedeni namen bomo dosegli s sistemom za certificiranje elektronske pošte, ki obsega terminalno napravo pošiljatelja elektronske pošte, ki jo je mogoče medsebojno povezati s strežnikom za odhodno elektronsko pošto, ki ga je mogoče povezati s strežnikom za dohodno elektronsko pošto, s katerim je nato mogoče povezati terminalno napravo prejemnika elektronske pošte, pri čemer je po izumu princip oziroma načelo delovanja tako, da je strežnik za odhodno elektronsko pošto mogoče povezati s strežnikom kvalificiranega organa za certificiranje, pri čemer strežnik kvalificiranega organa za certificiranje obsega notranji generator časa.

Prednost sistema po izumu je, da omogoča objektivno in nedvoumno potrjevanje vsebine in časa pošiljanja elektronske pošte.

Po prednostni izvedbi se na nižji ravni terminalne naprave pošiljatelja elektronske pošte uredi lasten strežnik pošiljatelja za odhodno pošto pošiljatelja.

V prednostni izvedbi strežnik za odhodno elektronsko pošto obsega blok za obdelavo kontrolne vsote e-poštnega sporočila (vsote e-poštnih sporočil), čemur zaporedno sledita blok za shranjevanje sporočila s časovnim žigom in blok za standardno pošiljanje obdelanega sporočila, medtem ko sta blok za obdelavo kontrolne vsote e-poštnega sporočila in blok za shranjevanje sporočila s časovnim žigom medsebojno



povezana z notranjim generatorjem časa na strežniku kvalificiranega organa za certificiranje.

V naslednji prednostni izvedbi se nahaja blok za avtorizacijo e-poštnega sporočila na strežniku za odhodno elektronsko pošto, in sicer pred blokom za obdelavo kontrolne vsote e-poštnega sporočila, pri čemer je blok za avtorizacijo e-poštnega sporočila medsebojno povezan, prek podatkovne zbirke uporabnikov storitve, s podatkovno zbirko dnevnika časovnih žigov, ki se nahaja na strežniku kvalificiranega organa za certificiranje.

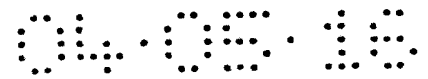
V naslednji prednostni izvedbi se na strežniku za odhodno elektronsko pošto, za blokom za shranjevanje sporočila s časom žigom, zaporedno nahajata blok za preverjanje integritete e-poštnega sporočila in shranjevanje podatkov, medtem ko je periferna naprava za uporabniško preverjanje elektronskega žiga medsebojno povezana z notranjim generatorjem časa na strežniku kvalificiranega organa za certificiranje. Periferno napravo za uporabniško preverjanje elektronskega žiga je mogoče medsebojno povezati tako s terminalno napravo pošiljatelja kot s shranjevanjem podatkov.

Kratek opis skic

Trije primeri ureditev sistema za certificiranje elektronske pošte so shematično prikazani na slikah 1, 2, 3 in 4.

Opis prednostnih izvedb

Primer izvedbe osnovne ureditve sistema za certificiranje elektronske pošte po izumu v skladu s sliko 1 obsega terminalno napravo 1 pošiljatelja elektronske pošte, ki lahko obsega katera koli oziroma vsa znana tehnična sredstva za pošiljanje in prejemanje elektronske pošte, npr. mobilni telefon, tablični računalnik, osebni računalnik z operacijskim sistemom Windows, Apple Macintosh, Linux, Android itd.



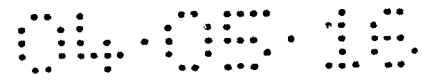
Terminalno napravo 1 pošiljatelja elektronske pošte je mogoče medsebojno povezati s strežnikom 16 za odhodno elektronsko pošto s pomočjo povezave 2 pošiljatelja prek interneta (ADSL, GSM, WiFi). V predstavljenem primeru izvedbe ima strežnik 16 za odhodno elektronsko pošto naslednje parametre: CPU E5-2603 2,4 GHz, RAM 16 GB, HDD 2x 500 GB SATA. Strežnik 16 za odhodno elektronsko pošto uporablja protokol „Simple Mail Transfer Protocol“ (skrajšano SMTP).

Strežnik 16 za odhodno elektronsko pošto je mogoče, s pomočjo povezave 12 prejemnika prek interneta, medsebojno povezati s strežnikom 13 za dohodno elektronsko pošto, ki ima v predstavljenem primeru izvedbe naslednje parametre: CPU E5-2603 2,4 GHz, RAM 16 GB, HDD 2x 500 GB SATA. Strežnik 13 za dohodno elektronsko pošto uporablja protokol POP3 ali IMAP za dostop naslovnika do sporočila.

S strežnikom 13 za dohodno elektronsko pošto je mogoče povezati s terminalno napravo 14 prejemnika elektronske pošte, ki obsega, podobno kot terminalna naprava 1 pošiljatelja elektronske pošte, katera koli oziroma vsa znana tehnična sredstva za pošiljanje in prejemanje elektronske pošte, npr. mobilni telefon, tablični računalnik, osebni računalnik z operacijskim sistemom Windows, Apple Macintosh, Linux, Android itd.

Strežnik 16 za odhodno elektronsko pošto je mogoče medsebojno povezati s strežnikom 17 kvalificiranega organa za certificiranje, ki obsega notranji generator časa 8. V predstavljenem primeru izvedbe strežnik 17 kvalificiranega organa za certificiranje upravlja podjetje Česká pošta s.p. in ima naslednje parametre: CPU E5-2603 2,4 GHz, RAM 16 GB, HDD 2x 500 GB SATA. Jasno je, da lahko tudi drugi subjekti, ki bodo izpolnjevali vnaprej določene zahteve in pridobili ustrezno dovoljenje, delujejo kot kvalificirani organ za certifikacijo.

Strežnik 16 za odhodno elektronsko pošto obsega blok 6 za obdelavo kontrolne vsote e-poštnega sporočila (izvedeno z uporabo strojne opreme CPU 2x E5-2620 2,0 GHz, RAM 64 GB, HDD 2x 2 TB SATA), čemur zaporedno sledita blok 7 za



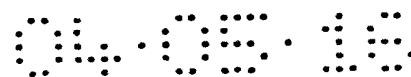
shranjevanje sporočila s časovnim žigom (izvedeno z uporabo strojne opreme CPU E5-2603 2,4 GHz, RAM 16 GB, HDD 2x 500 GB SATA) in blok 11 za standardno pošiljanje obdelanega sporočila (izvedeno z uporabo strojne opreme CPU E5-2603 2,4 GHz, RAM 16 GB, HDD 2x 500 GB SATA). Blok 6 za obdelavo kontrolne vsote e-poštnega sporočila in blok 7 za shranjevanje sporočila s časovnim žigom sta medsebojno povezana z notranjim generatorjem časa 8 na strežniku 17 kvalificiranega organa za certificiranje.

Po pošiljanju elektronske pošte iz katere koli terminalne naprave 1 pošiljatelj elektronske pošte prek povezave 2 uporabnika na strežnik 16 za izhodno pošto, blok 6 za obdelavo kontrolne vsote e-poštnega sporočila izračuna kontrolno vsoto, ki se imenuje „hash“ (slo., kontrolna vsota), ki se nato pošlje na strežnik 17 kvalificiranega organa za certificiranje, kjer se v notranjem generatorju časa 8 e-poštnemu sporočilu doda časovni žig, nato pa se e-poštno sporočilo s časovnim žigom pošlje v blok 7 za shranjevanje sporočila s časovnim žigom.

E-poštno sporočilo, ki je obdelano na tak način, se pošlje na strežnik 13 za dohodno elektronsko pošto prek bloka 11 za standardno pošiljanje in prek povezave 12 prejemnika, nato pa se pošlje s strežnika za dohodno pošto na terminalno napravo 14 prejemnika.

Na osnovi nastavitve storitve se lahko pošiljatelju na stopnji bloka 7 za shranjevanje sporočila pošlje potrdilo o pošiljanju sporočila.

Naslednji primer izvedbe ureditve sistema za certificiranje elektronske pošte v skladu s sliko 2 se razlikuje od primera izvedbe s slike 1 po tem, da se na strežniku 16 za odhodno elektronsko pošto, pred blokom 6 za obdelavo kontrolne vsote e-poštnega sporočila, nahaja blok 3 za avtorizacijo e-poštnega sporočila (izvedeno z uporabo strojne opreme CPU E5-2603 2,4 GHz, RAM 16 GB, HDD 2x 500 GB SATA), ki je, prek podatkovne zbirke uporabnikov storitve 4 (izvedeno z uporabo strojne opreme CPU E5-2603 2,4 GHz, RAM 16 GB, HDD 2x 500 GB SATA in sistema za upravljanje podatkovnih zbirk MS SQL), medsebojno povezan s podatkovno zbirko 5

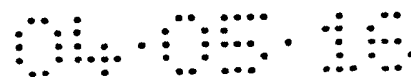


dnevnika časovnih žigov (izvedeno z uporabo strojne opreme CPU E5-2603 2,4 GHz, RAM 16 GB, HDD 2x 500 GB SATA in sistema za upravljanje podatkovnih zbirk MS SQL) na strežniku 17 kvalificiranega organa za certificiranje.

Elektronska pošta se pošlje iz katere koli terminalne naprave 1 pošiljatelja elektronske pošte prek povezave 2 pošiljatelja na strežnik 16 za izhodno pošto, pri čemer se, s pomočjo bloka 3 za avtorizacijo e-poštnega sporočila, podatkovne zbirke 4 uporabnikov storitev in podatkovne zbirke 5 dnevnika časovnih žigov, preverijo uporabniška pooblastila osebe, ki zahteva certificiranje elektronske pošte. Nadaljnja obdelava e-poštnega sporočila je enaka kot v primeru izvedbe s slike 1, ki je opisan zgoraj.

Naslednji primer izvedbe ureditve sistema za certificiranje elektronske pošte v skladu s sliko 3 se razlikuje od primera izvedbe s slike 1 po tem, da se na strežniku 16 za odhodno elektronsko pošto, za blokom 7 za shranjevanje sporočila s časovnim žigom, zaporedno razporejena nahajata blok 9 za preverjanje integritete e-poštnega sporočila (izvedeno z uporabo strojne opreme CPU E5-2603 2,4 GHz, RAM 16 GB, HDD 2x 500 GB SATA) in shranjevanje podatkov 10 (izvedeno z uporabo strojne opreme CPU E5-2603 1,8 GHz, RAM 16 GB, HDD 24x WD RED RAID EDITON 3 TB SATA). Periferna naprava 15 za uporabniško preverjanje elektronskega žiga (npr. mobilni telefon, tablični računalnik, osebni računalnik) je medsebojno povezana z notranjim generatorjem časa 8 na strežniku 17 kvalificiranega organa za certificiranje, medtem ko je periferna naprava 15 za uporabniško preverjanje elektronskega žiga medsebojno povezana tako s terminalno napravo 1 pošiljatelja elektronskega sporočila kot tudi s shranjevanjem podatkov 10.

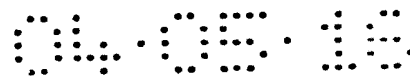
Obdelava e-poštnega sporočila je enaka kot v zgoraj navedenem primeru izvedbe s slike 1. Dodatek bloka 9 za preverjanje integritete e-poštnega sporočila in shranjevanje podatkov 10 v kombinaciji s periferno napravo 15 za uporabniško preverjanje elektronskega žiga omogočajo, zraven funkcij, opisanih v zvezi z izvedbo v skladu s sliko 1, preverjanje shranjenih podatkov glede doslednosti in preverjanje veljavnosti časovnega žiga, skupaj s celotnim shranjevanjem sporočila, kakor tudi



naknadno preverjanje procesa dostave sporočila na ravni strežnika 16 za odhodno pošto in strežnika 13 za dohodno pošto. To preverjanje se lahko izvede tudi s strani pošiljatelja sporočila neodvisno od upravljavca strežnika 16 za odhodno pošto s pomočjo periferne naprave 15 za uporabniško preverjanje elektronskega žiga. Shranjevanje podatkov 10 e-poštnega sporočila, časovnega žiga sporočila in drugih atributov se uporablja za shranjevanje celotnega nabora podatkov, ki so povezani s poslanim sporočilom, kar dodatno omogoča dostop pošiljatelja sporočila in preverjanje ali delo s shranjenimi sporočili v skladu z opredeljenimi pravili.

Naslednji primer izvedbe ureditve sistema za certificiranje elektronske pošte v skladu s sliko 4 se razlikuje od primera izvedbe s slike 1 po tem, da ima pošiljatelj svoj strežnik 18 za odhodno pošto pošiljatelja (izvedeno z uporabo strojne opreme CPU 2x E5-2620 2,0 GHz, RAM 64 GB, HDD 2x 2 TB SATA). Strežnik 16 za odhodno elektronsko pošto se izvaja kot relejski strežnik SMTP, ki je nadrejen uporabnikovemu lastnemu strežniku 18 za odhodno pošto uporabnika. Sporočilo se pošlje s terminalne naprave 1 pošiljatelja elektronske pošte na strežnik 16 za odhodno elektronsko pošto prek pošiljateljevega lastnega strežnika 18 za odhodno pošto pošiljatelja. Nadaljnja obdelava e-poštnega sporočila je nato enaka kot v primeru izvedbe s slike 1, ki je opisan zgoraj.

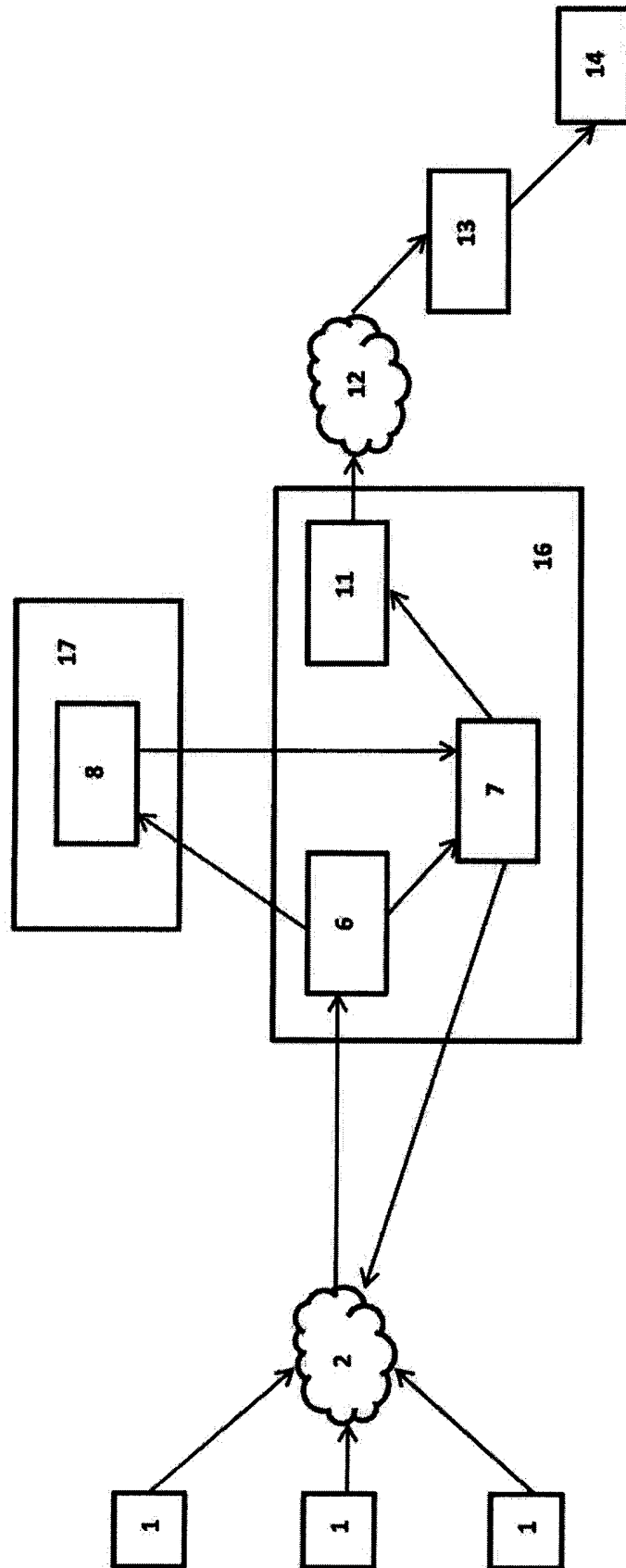
- 1 terminalna naprava pošiljatelja elektronske pošte
- 2 povezava pošiljatelja
- 3 blok za avtorizacijo e-poštnega sporočila
- 4 podatkovna zbirka uporabnikov storitve
- 5 podatkovna zbirka dnevnika časovnih žigov
- 6 blok za obdelavo kontrolne vsote e-poštnega sporočila
- 7 blok za shranjevanje sporočila s časovnim žigom
- 8 notranji generator časa
- 9 blok za preverjanje integritete e-poštnega sporočila
- 10 shranjevanje podatkov
- 11 blok za standardno pošiljanje obdelanega sporočila
- 12 povezava prejemnika
- 13 strežnik za dohodno elektronsko pošto
- 14 terminalna naprava prejemnika
- 15 periferna naprava za uporabniško preverjanje elektronskega žiga
- 16 strežnik za odhodno elektronsko pošto
- 17 strežnik kvalificiranega organa za certificiranje
- 18 lasten strežnik pošiljatelja za odhodno pošto pošiljatelja



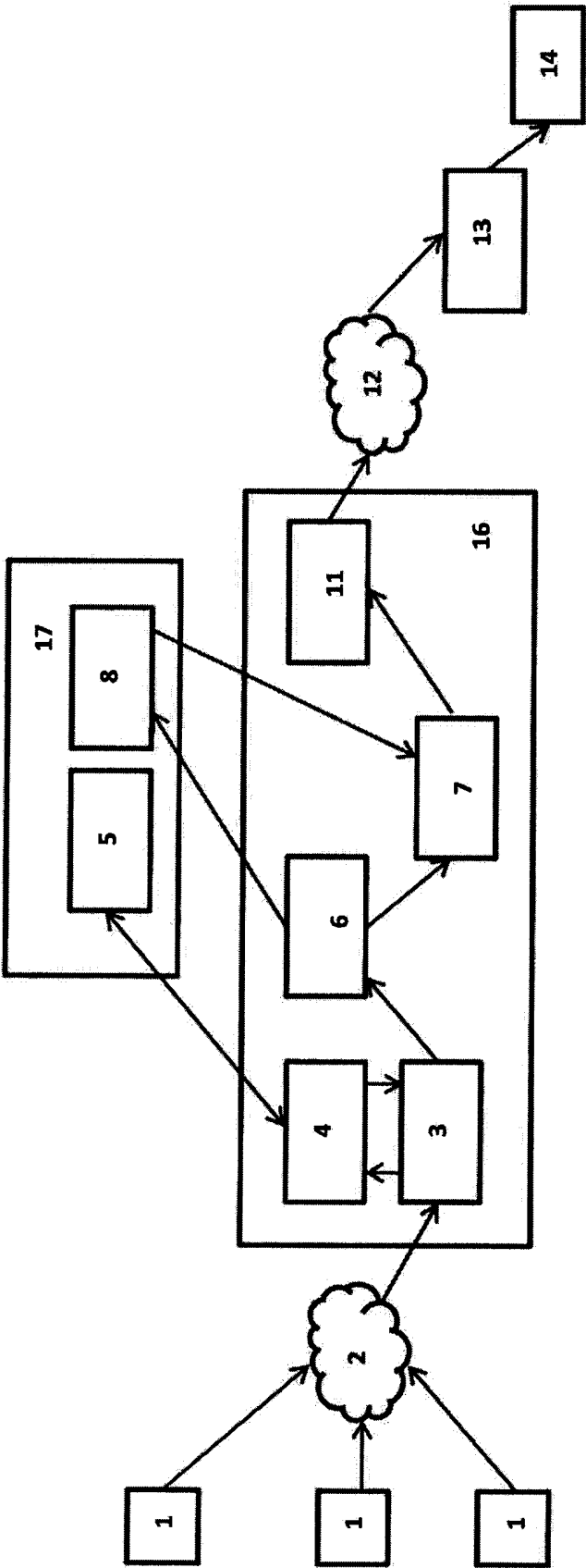
PATENTNI ZAHTEVKI

1. Sistem za certificiranje elektronske pošte, ki obsega terminalno napravo (1) pošiljatelja elektronske pošte, ki jo je mogoče medsebojno povezati s strežnikom za odhodno elektronsko pošto (16), ki ga je mogoče povezati s strežnikom za dohodno elektronsko pošto (13), na katerega je nato mogoče povezati terminalno napravo (14) prejemnika elektronske pošte, **označen s tem**, da je strežnik za odhodno elektronsko pošto (16) mogoče medsebojno povezati s strežnikom (17) kvalificiranega organa za certificiranje, pri čemer strežnik (17) kvalificiranega organa za certificiranje obsega notranji generator časa (8).
2. Sistem za certificiranje elektronske pošte po zahtevku 1, **označen s tem**, da je za terminalno napravo (1) pošiljatelja elektronske pošte urejen pošiljatelj lastni strežnik (18) za odhodno pošto.
3. Sistem za certificiranje elektronske pošte po zahtevku 2, **označen s tem**, da strežnik za odhodno elektronsko pošto (16) obsega blok (6) za obdelavo kontrolne vsote e-poštnega sporočila, čemur zaporedno sledita blok (7) za shranjevanje sporočila s časovnim žigom in blok (11) za standardno pošiljanje obdelanega sporočila, pri čemer sta blok (6) za obdelavo kontrolne vsote e-poštnega sporočila in blok (7) za shranjevanje sporočila s časovnim žigom medsebojno povezana z notranjim generatorjem časa (8) na strežniku (17) kvalificiranega organa za certificiranje.
4. Sistem za certificiranje elektronske pošte po zahtevku 2 ali 3, **označen s tem**, da se blok za avtorizacijo e-poštnega sporočila (3) nahaja na strežniku za odhodno elektronsko pošto (16), in sicer pred blokom (6) za obdelavo kontrolne vsote e-poštnega sporočila, pri čemer je blok za avtorizacijo e-poštnega sporočila (3) medsebojno povezan, prek podatkovne zbirke (4) uporabnikov storitve, s podatkovno zbirko (5) dnevnika časovnih žigov, ki se nahaja na strežniku (17) kvalificiranega organa za certificiranje.

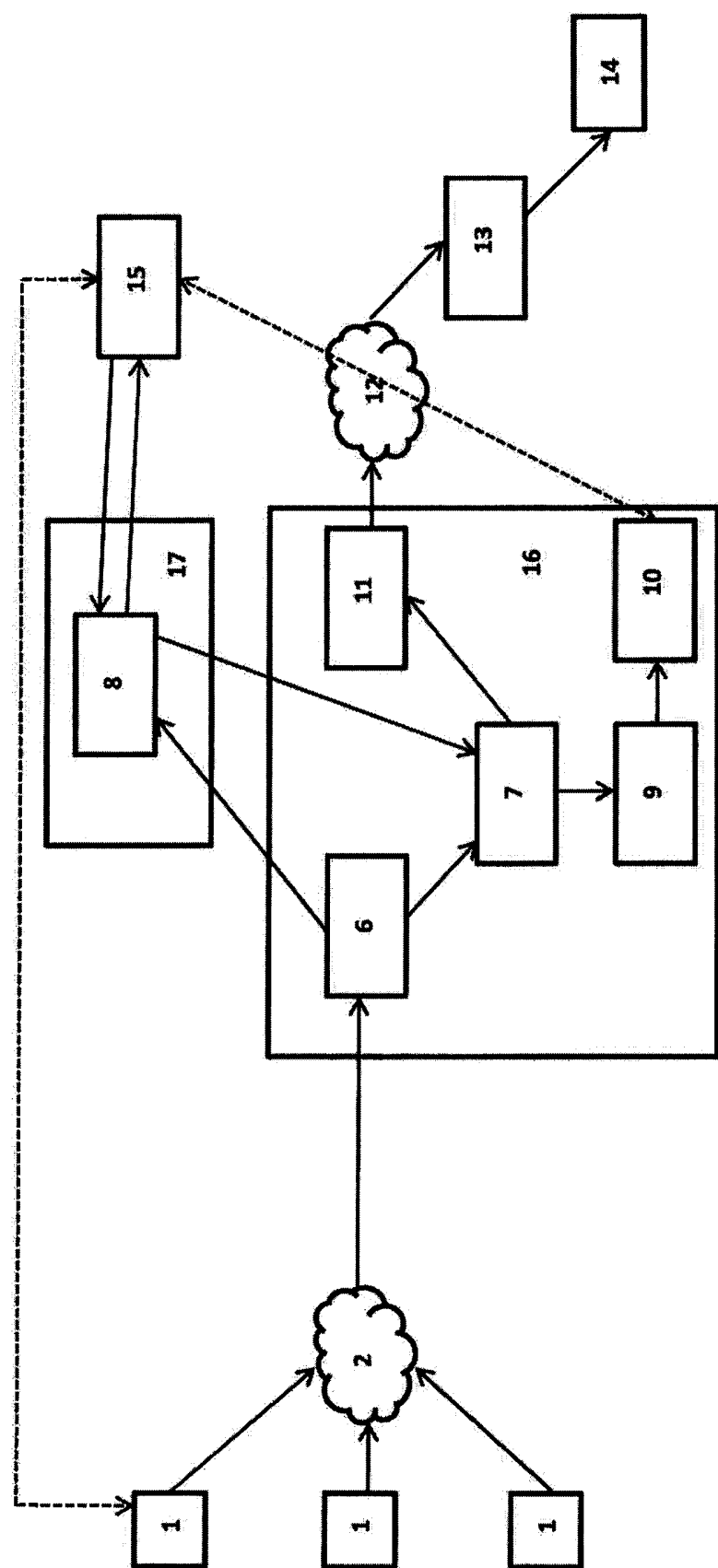
5. Sistem za certificiranje elektronske pošte po zahtevku 2 ali 3, **označen s tem**, da se na strežniku (16) za odhodno elektronsko pošto, za blokom (7) za shranjevanje sporočila s časovnim žigom, nahajata blok (9) za preverjanje integritete e-poštnega sporočila in shranjevanje podatkov (10), pri čemer je periferna naprava (15) za uporabniško preverjanje elektronskega žiga medsebojno povezana z notranjim generatorjem časa (8) na strežniku (17) kvalificiranega organa za certificiranje, pri čemer je mogoče periferno napravo (15) za uporabniško preverjanje elektronskega žiga medsebojno povezati tako s terminalno napravo (1) pošiljatelja kot s shranjevanjem podatkov (10).



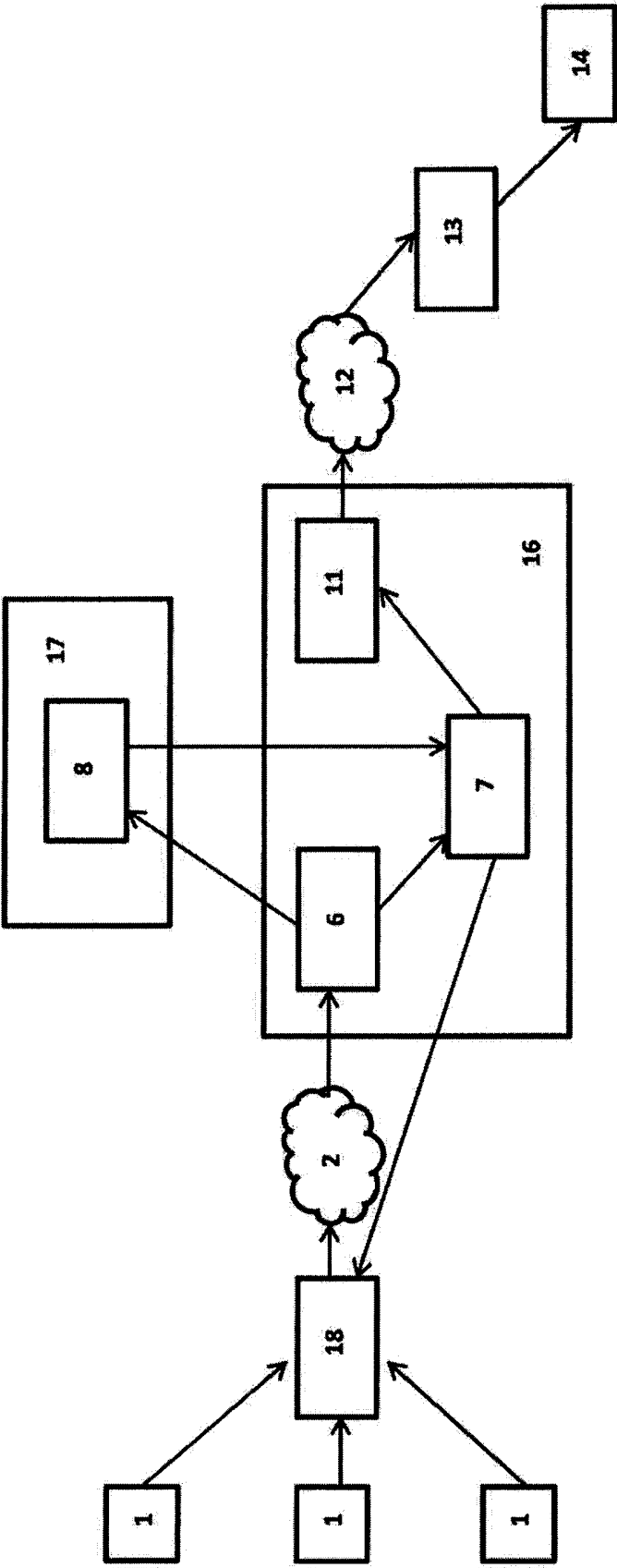
Sl. 1



SI. 2



SI. 3



Sl. 4