PŘIHLÁŠKA VYNÁLEZU

zveřejněná podle § 31 zákona č. 527/1990 Sb.

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(22) Přihlášeno: **12.10.2007**

(40) Datum zveřejnění přihlášky vynálezu: **22.04.2009**
(Věstník č. 16/2009)

(21) Číslo dokumentu:
2007-713

(13) Druh dokumentu: **A3**

(51) Int. Cl.:
G06F 21/00 (2006.01)

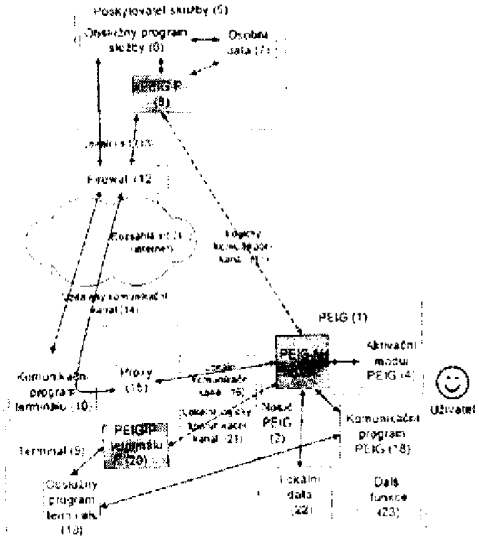
(71) Přihlašovatel:
ANECT, a. s., Brno, CZ

(72) Původce:
Neumann Libor Ing. CSc., Praha 5, CZ

(74) Zástupce:
Doc. Ing.CSc. Jindřich Špaček, patentový zástupce, Svatopluka Čecha 106a, Brno, 61200

(54) Název přihlášky vynálezu:

Způsob navazování chráněné elektronické komunikace mezi různými elektronickými prostředky, zejména mezi elektronickými prostředky poskytovatelů elektronických služeb a elektronickými prostředky uživatelů elektronických služeb



(57) Anotace:

Jedná se o způsob navazování chráněné elektronické komunikace různými elektronickými prostředky, zejména mezi elektronickými prostředky poskytovatelů elektronických služeb a elektronickými prostředky uživatelů elektronických služeb a/nebo mezi lokálními elektronickými prostředky a elektronickými prostředky uživatelů elektronických služeb. Uživatelé elektronických služeb se nejprve vybaví osobním nosičem elektronické identity bez informací o identitě uživatele. Při prvním připojení prázdného osobního nosiče uživatele na elektronické prostředky libovolného poskytovatele služeb a/nebo na lokální elektronické prostředky, si osobní nosič elektronické identity a elektronické prostředky poskytovatele služeb a/nebo lokální elektronické prostředky vzájemně vygenerují ověřitelnou elektronickou identitu, která se v osobním nosiči elektronické identity a v elektronických prostředcích poskytovatele služeb a/nebo v lokálních elektronických prostředcích uloží pro potřeby další vzájemné elektronické komunikace, odděleně od ostatních identit a bez znalosti osobních údaju o uživateli elektronických služeb. Následně se jen vygenerované a uložené informace využijí k ověření identity při každém dalším připojení uživatele elektronických služeb na elektronické prostředky toho kterého poskytovatele služeb a/nebo na lokální elektronické prostředky.

CZ 2007 - 713 A3

Způsob navazování chráněné elektronické komunikace mezi různými elektronickými prostředky, zejména mezi elektronickými prostředky poskytovatelů elektronických služeb a elektronickými prostředky uživatelů elektronických služeb

Oblast techniky

Vynález se týká způsobu navazování chráněné elektronické komunikace mezi různými elektronickými prostředky, zejména mezi elektronickými prostředky poskytovatelů elektronických služeb a elektronickými prostředky uživatelů elektronických služeb a/nebo mezi lokálními elektronickými prostředky a elektronickými prostředky uživatelů elektronických služeb.

Stávají stav techniky

Známé systémy pro elektronickou komunikaci, zejména mezi elektronickými prostředky poskytovatelů elektronických služeb a elektronickými prostředky uživatelů elektronických služeb si vyžadují přímou manipulaci uživatele s informacemi používanými v určování nebo/a ověřování jeho elektronické identity zadáváním identifikátorů, například uživatelských jmen, ověřováním identity pomocí hesla, vkládáním PIN apod.

Zcela obvyklé je, že do systémů, kromě uživatele a poskytovatele služby, vstupují třetí strany a další subjekty zapojené do vytváření, ověřování, používání, zneplatnění či pro jiné manipulace s elektronickou identitou, například certifikační nebo registrační autority, poskytovatelé služeb elektronické identity – Identity Service Provider apod.

Řečené systémy využívají části či všechny informace, kterými uživatel ověřuje svoji fyzickou identitu pro vytvoření nebo ověření elektronické identity a k dalším činnostem přímo spojených s elektronickou identitou.

Nevýhodami známých systémů pro elektronickou komunikaci mezi elektronickými prostředky poskytovatelů elektronických služeb zůstává, že osobní údaje uživatele elektronických služeb a další informace týkající se osoby uživatele, nejsou odděleny od jeho elektronické identity. Protože identifikátory nejsou anonymní, znamená to, že identifikátory obsahují informace, pomocí nichž je možné přímo nebo nepřímo zjistit totožnost uživatele, jméno nebo část jména, rodné číslo či jiné osobní údaje, pomocí kterých lze určit či odhadnout, která fyzická osoba identifikátor používá, jaké a jak služby poskytovatele služeb používá a také jaké a jak používá služby jakého jiného poskytovatele služeb, což značí, že

uživatel není dostatečně chráněn před neoprávněným shromažďováním informací o své identitě a o svém jednání.

Dalšími nevýhodami známých systémů je komplikované ovládání jejich uživateli, nutnost vytvářet a pamatovat si množství hesel, PIN či dalších údajů nutných k ověření elektronické identity a přitom zachování jejich důvěrnosti a ochránit je proti zneužití. To často vede v k situaci, že uživatel tyto informace zapomene nebo prozradí neoprávněné osobě a tyto situace je nutné komplikovaně řešit. Tyto nevýhody se v praxi objevují jako obzvláště komplikující, pokud uživatel elektronických služeb komunikuje s velkým množstvím poskytovatelů elektronických služeb a/nebo poskytovatel elektronických služeb komunikuje s velkým počtem uživatelů služeb, zejména ze vzdálených lokalit.

Také existence třetích stran a jejich zapojení do vytváření, ověřování, zneplatnění či pro jiné manipulace s elektronickou identitou je komplikujícím prvkem jak pro uživatele elektronických služeb, tak pro poskytovatele elektronických služeb, často spojený i s dalšími náklady a poplatky.

Podstata vynálezu

Cílem vynálezu je odstranění uvedených nevýhod a to novým způsobem navazování chráněné elektronické komunikace mezi různými elektronickými prostředky, zejména mezi elektronickými prostředky poskytovatelů elektronických služeb a elektronickými prostředky uživatelů elektronických služeb a/nebo mezi lokálními elektronickými prostředky a elektronickými prostředky uživatelů elektronických služeb, spočívajícím v tom, že se uživatelé elektronických služeb nejprve vybaví osobním nosičem elektronické identity bez informací o identitě uživatele, načež až při prvním připojení prázdného osobního nosiče uživatele na elektronické prostředky libovolného poskytovatele služeb a/nebo na lokální elektronické prostředky, si osobní nosič elektronické identity a elektronické prostředky poskytovatele služeb a/nebo lokální elektronické prostředky vzájemně vygenerují ověřitelnou elektronickou identitu, která se v osobním nosiči elektronické identity a v elektronických prostředcích poskytovatele služeb a/nebo v lokálních elektronických prostředcích uloží pro potřeby další vzájemné elektronické komunikace, odděleně od ostatních identit a bez znalostí osobních údajů o uživateli elektronických služeb, přičemž následně se jen vygenerované a uložené informace využijí k ověření identity při každém dalším připojení uživatele elektronických služeb na elektronické prostředky toho kterého poskytovatele služeb a/nebo na lokální elektronické prostředky.

Podle vynálezu se dále jeví výhodné, že se uložené informace využijí k ověření identity při každém dalším připojení uživatele elektronických služeb na elektronické prostředky tohoto poskytovatele služeb a/nebo na lokální elektronické prostředky před každou změnou ověřitelné elektronické identity, při které je identifikátor nahrazen jiným identifikátorem bez ztráty identity a personifikovaného kontextu.

Podle vynálezu se zvláště jeví výhodné, že po poskytnutí osobních údajů elektronickým prostředkům poskytovatele služeb a/nebo lokálnímu elektronickému prostředku a souhlasu uživatele služeb s jejich předáním alespoň elektronickým prostředkům jednoho dalšího poskytovatele služeb a/nebo lokálnímu elektronickému prostředku se osobním nosičem elektronické identity spolu s elektronickými prostředky zúčastněných poskytovatelů služeb a/nebo spolu s lokálními elektronickými prostředky vygeneruje přechodná jednoúčelová elektronická identita určená k realizaci předání osobních dat uživatele mezi zúčastněnými poskytovateli služeb a/nebo lokálními elektronickými prostředky.

Z hlediska vytváření tvorby elektronické identity se podle vynálezu dále jeví výhodné, že vytváření ověřitelné elektronické identity a ověřování identity se provádí symetricky tak, že kombinací jedné části identifikátoru generovanou osobním nosičem elektronické identity a druhé části identifikátoru generovanou elektronickými prostředky poskytovatelů elektronických služeb nebo lokálními elektronickými prostředky vznikne identifikátor, který ani jedna strana nemůže bez spolupráce druhé strany vytvořit nebo ověřit, přičemž osobní nosič elektronické identity ověřuje identitu na straně uživatele pomocí tajné informace spojené s identitou, předávané elektronickými prostředky poskytovatelů elektronických služeb nebo lokálními elektronickými prostředky, a naopak elektronické prostředky poskytovatelů elektronických služeb nebo lokální elektronické prostředky ověřují identitu na straně poskytovatele služeb nebo na straně lokálního elektronického prostředku pomocí tajné informace spojené s identitou, předávané osobním nosičem elektronické identity, načež teprve po úspěšném ověření identifikátorů obou stran je identita považována za ověřenou.

Z hlediska ochrany osobních údajů je podle vynálezu výhodné, že provádění asymetrické kryptografie se standardními páry klíčů se uskutečňuje s vypuštěním všech datových struktur obsahujících osobní údaje a s vypuštěním postupů a činností spojených s těmito osobními údaji.

Pro zvýšení bezpečnosti je podle vynálezu dále výhodné, že se nesprávnou nebo neúspěšnou aktivací osobního nosiče elektronické identity může spustit samodestrukční mechanismus pro zrušení platnosti identifikace obsažené jak v osobním nosiči elektronické identity na straně uživatele, tak v elektronických prostředcích poskytovatelů elektronických služeb a/nebo lokálních elektronických prostředcích na straně poskytovatele služeb a/nebo lokálních elektronických prostředků.

Přehled obrázků na výkresech

Další výhody a účinky vynálezu jsou patrné z přiložených obrázků, kde značí:

obr.1 zobrazení procesu navazování chráněné elektronické komunikace mezi různými elektronickými prostředky, zejména mezi elektronickými prostředky poskytovatelů elektronických služeb a elektronickými prostředky uživatelů elektronických služeb a/nebo mezi lokálními elektronickými prostředky a elektronickými prostředky uživatelů elektronických služeb prostřednictvím logických komunikačních kanálů a osobního nosiče elektronické identity PEIG (Personal Electronic Identity Gadget),

obr. 2 demonstrování příkladu řetězení systému s vícenásobným až neomezeným počtem partnerů vytvořením jen potřebného počtu logických komunikačních kanálů mezi osobními nosiči elektronické identity PEIG a elektronickými prostředky poskytovatelů elektronických služeb a/nebo lokálními elektronickými prostředky.

Příklad provedení vynálezu

Způsob navazování chráněné elektronické komunikace podle vynálezu, mezi různými elektronickými prostředky, zejména mezi elektronickými prostředky poskytovatelů elektronických služeb a elektronickými prostředky uživatelů elektronických služeb, je založen na automatizovaném speciálním zařízení PEIG 1 (Personal Electronic Identity Gadget – osobní nosič elektronické identity). Jedná se o automatizované specielní elektronické zařízení nebo část zařízení univerzálně využívané svým vlastníkem-uživatelem pro všechny činnosti spojené s elektronickou identitou.

Zařízení PEIG 1 je určeno k osobnímu používání jednou osobou, tedy k uchování a obsluze elektronické identity svého vlastníka-uživatele a k zajištění veškerých dalších činností spojených se vznikem, užíváním, údržbou a zrušením elektronické identity nebo identit jediného uživatele.

Elektronické zařízení, vykonávající funkce PEIG 1, které může vykonávat i další funkce je nazýváno nosič PEIG 2. Jde o malé a snadno přenosné zařízení, umožňující vlastníkovi-uživateli nosit svoji elektronickou identitu stále s sebou. Významnou vlastností zařízení je extrémně jednoduché používání. Vlastnictví a užívání PEIG 1 je dobrovolné a jedna osoba smí vlastnit a užívat i více PEIG 1.

Aktivace PEIG 1 je oddělena od elektronické identity. Data užívaná pro aktivaci PEIG 1 nejsou používána pro elektronickou identitu a naopak, data užívaná pro elektronickou identitu nejsou užívána k aktivaci PEIG 1.

PEIG 1 je sám o sobě nerozlišitelný od jiných PEIG pracujících v daném systému. Je vyráběn prázdný, bez jakékoli elektronické identity a bez informací potřebných k personifikované aktivaci PEIG.

Zařízení PEIG 1 minimálně obsahuje dvě vzájemně oddělené části, které spolu jsou propojeny. Jedná se o PEIG-M 3 a Aktivační modul PEIG 4.

Modul PEIG-M 3 zajišťuje veškeré činnosti spojené s elektronickou identitou na straně uživatele.

Aktivační modul PEIG 4 slouží k aktivaci a deaktivaci prostředků elektronické identity vlastníkem PEIG. Aktivační modul PEIG 4 komunikuje s uživatelem tak, aby ověřil fyzickou identitu uživatele zvoleným způsobem, například snímáním otisků prstů, oční zornice, vyplněním hesla apod.

Kromě výše popsaných modulů může nosič PEIG 2 obsahovat i další moduly sloužící k využívání elektronické identity v různých situacích přímo prostřednictvím Nosiče PEIG 2, jako je například komunikační program PEIG 18.

Nosič PEIG 2 může obsahovat i Lokální data 22, tedy data, která uživatel nosí s sebou spolu s PEIG 1. Přístup k Lokálním datům 22 může být řízen na základě informací z PEIG-M 3, tedy může být umožněn jen vybraným Poskytovatelům služeb 5.

Kromě toho může nosič PEIG 2 obsahovat i další moduly sloužící k jiným účelům, na obr. 1 vyznačeno jako Další funkce 23.

PEIG 1 komunikuje s Poskytovatelem služby 5. Jedná se o zařízení určená k poskytování elektronických služeb. Tato zařízení zpravidla obsahují řadu modulů sloužících k různým účelům více či méně těsně spojeným s poskytovanou službou a

s elektronickou identitou uživatele služby. Jedná se např. o Obslužný program služby 6 a o úložiště osobních a jiných údajů o uživatelích služby Osobní data 7.

Modul PEIG-P 8 u Poskytovatele služby 5 zajišťuje veškeré činnosti spojené s vznikem, užíváním, údržbou a zrušením elektronické identity identit uživatelů služby či souboru služeb.

Modul PEIG-P 8 na straně Poskytovatele služeb 5 komunikuje logicky přímo s modulem PEIG-M 3 na straně uživatele prostřednictvím Logického komunikačního kanálu 17. Vzájemně si vyměňují, potvrzují, mění, ověřují a jinak manipulují s informacemi spojenými s elektronickou identitou uživatele.

Vlastní fyzická výměna informací probíhá prostřednictvím řady různých modulů, služeb a zařízení tak, aby byla zajištěna vzájemná komunikace při zachování potřebných vazeb a potřebné úrovně zabezpečení komunikace. K tomu je používáno, jak níže uvedeno, běžně dostupných a v praxi používaných prostředků a také specielních prostředků, z nichž některé jsou sdíleny i pro jiné účely a některé jsou využity specielně pro komunikaci spojenou s elektronickou identitou.

Uživatel běžně komunikuje pomocí Terminálu 9. To je běžné zařízení určené k elektronické komunikaci s elektronickými službami. Příkladem realizace takového terminálu může být osobní počítač PC nebo samoobslužný veřejný terminál s potřebným programovým vybavením. Vlastní komunikaci uživatele zajišťuje Komunikační program terminálu 10, který komunikuje s Obslužným programem služby 6. K tomu užívá kromě prostředků Terminálu 9 a Poskytovatele služeb 5 také další prostředky a služby. Jedná se zejména o prostředky přenosu dat, Rozsáhlé sítě 11, například Internetu, ochranné funkce Firewallu 12 a služeb Lokální sítě 13. Ochranné funkce modulu Firewall 12 mohou být realizovány různým způsobem. Nemusí jít vždy o funkčnost firewallu jako takového, mohou být užity i jiné způsoby ochrany vnitřních sítí poskytovatele služby, například Proxy serveru.

Obslužný program služby 6 u Poskytovatele služby 5 využívá ke své činnosti informaci o elektronické identitě uživatele od PEIG-P 8 a pomocí těchto informací získává další údaje o uživateli, např. Osobní data 7.

K tomu aby PEIG-P 8 měl k dispozici správné a bezpečné informace o elektronické identitě uživatele, komunikuje s PEIG-M 3. Využívá k tomu shodných nebo podobných komunikačních prostředků jako komunikace mezi Komunikačním programem terminálu 10 a Obslužným programem služby 6, tedy kromě prostředků Terminálu 9 a Poskytovatele

služeb 5 také prostředky přenosu dat Rozsáhlé sítě 11, například Internetu, ochranné funkce Firewallu 12 a služeb Lokální sítě 13. Souhrnně jsou tyto prostředky označeny jako Vzdálený komunikační kanál 14. Tento Vzdálený komunikační kanál 14 umožňuje obousměrný přenos informací spojených s elektronickou identitou mezi prostředky Poskytovatele služeb 5 a Komunikačním programem terminálu 10 a to tak, že jsou jednoznačně svázány s komunikací poskytované elektronické služby příslušnému uživateli.

Komunikace mezi PEIG-P 8 a PEIG-M 3 je směrována běžnými prostředky na bezpečnostní modul Proxy 15 zpravidla pomocí Komunikačního programu terminálu 10. Bezpečnostní funkce modulu Proxy 15 může být zajištěna i jiným způsobem, například pomocí firewallu.

Bezpečnostní modul Proxy 15 komunikuje s modulem PEIG-M 3 s využitím prostředků lokální komunikace a lokálních komunikačních prostředků Terminálu 9 a Nosiče PEIG 2. Lokální komunikační prostředky, tedy komunikační prostředky Terminálu 9 a Nosiče PEIG 2, jsou běžné prostředky místní blízké komunikace mezi elektronickými zařízeními s vyhovujícími technickými i bezpečnostními parametry.

Těmito prostředky je dohromady vytvořen Lokální komunikační kanál 16, pomocí kterého dochází ke komunikaci přímo mezi PEIG-M 3 a Proxy 15.

Logický komunikační kanál 17, pomocí kterého dochází ke komunikaci přímo mezi PEIG-M 3 a PEIG-P 8 je vytvořen Vzdáleným komunikačním kanálem 14, Proxy 15, Lokálním komunikačním kanálem 16 a zpravidla také Komunikačním programem terminálu 10.

Příklady dalšího využití systému navazování chráněné elektronické komunikace mezi různými elektronickými prostředky

Lokální využití

PEIG 1 může sloužit také k zajištění a obsluze elektronické identity při lokální komunikaci uživatele s lokálními elektronickými prostředky zobrazenými jako Terminál 9. Při tom Terminál 9 může nebo nemusí komunikovat se vzdáleným Poskytovatelem služeb 5. V tomto případě bude uživatel používat Komunikační program PEIG 18 umístěný na Nosiči

PEIG 2. Tento Komunikační program PEIG 18 bude komunikovat s Obslužným programem terminálu 19.

PEIG-M 3 bude komunikovat přímo s PEIG-P terminálu 20 a to prostřednictvím Lokálního komunikačního kanálu 16 a vnitřních komunikačních prostředků Nosiče PEIG 2 a Terminálu 9, čímž vytvoří Lokální logický komunikační kanál 21. PEIG-P terminálu 20 předá informace o elektronické identitě uživatele Obslužnému programu terminálu 19 a ten pak i příslušným dalším modulům Terminálu 9.

Společné využívání

Prostředky elektronické identifikace jsou určeny k univerzálnímu použití velkým počtem uživatelů i poskytovatelů služeb 5. Proto jeden PEIG 1 může být použit jedním uživatelem-vlastníkem k elektronické identifikaci s více Poskytovateli služeb 5 a také jeden Poskytovatel služeb 5 může využít více různými PEIG 1 vlastněnými různými uživateli pro jejich identifikaci.

Funkčnost jednotlivých prostředků elektronické identifikace jak na straně uživatele PEIG 1 tak na straně Poskytovatele služeb 5 je uzpůsobena tomuto násobnému použití v principu s neomezeným počtem partnerů. Počet partnerů je omezen pouze parametry příslušného použitého vybavení, např. kapacitou paměti.

Při komunikaci mezi větším počtem uživatelů PEIG 1 a Poskytovatelů služeb 5 je vytvořen potřebný počet Logických komunikačních kanálů 17 (obr.2), které zajišťují v součinnosti s funkčností prostředků elektronické identity PEIG-M 3 a PEIG-P 8 jednoznačné vztahy mezi uživateli a poskytovanými službami. To platí analogicky i pro lokální využívání.

Prostředky elektronické identity PEIG-M 3 a PEIG-P 8 lze řetězit tak, že PEIG-P 8 je použit jako Aktivační modul PEIG 4 zřetězeného PEIG 1. Lze tak jedním PEIG 1 aktivovat další PEIG 1. Je možné zřetězit i různé typy prostředků elektronické identity. Zřetězením lze řešit různé situace lokální komunikace, případně vzdálené komunikace, např. při řešení součinnosti s dalšími systémy pro zajištění zpětné kompatibility či dosahu nebo napájení při bezdrátové komunikaci.

Funkce systému navazování chráněné elektronické komunikace a spolupráce PEIG-M a PEIG-P

Následující text popisuje vzájemnou součinnost PEIG-M 3 a PEIG-P 8, resp. PEIG-P terminálu 20, při práci s elektronickou identitou. V dalším textu je pojmem PEIG-P 8 popsán jak PEIG-P 8 Poskytovatele služeb 5 tak PEIG-P terminálu 20. Jejich spolupráce s PEIG-M 3 je shodná.

Při výrobě PEIG-M 3 ani PEIG-P 8 neobsahují žádné informace o elektronické identitě. Jsou prázdné.

Uživatel-vlastník aktivuje PEIG 1 zpravidla po předchozím nastavení Aktivačního modulu PEIG 4. Při prvním přístupu uživatele k poskytované službě dojde k vygenerování elektronické identity uživatele pro příslušnou službu vzájemnou součinností PEIG-M 3 a PEIG-P 8. Příslušné informace jsou uschovány uvnitř PEIG-M 3 a PEIG-P 8.

Při dalším pokusu o přístup uživatele k poskytované službě jsou informace uložené v PEIG-M 3 a PEIG-P 8 použity k odlišení uživatele služby a ověření elektronické identity uživatele.

V případě potřeby jsou bezpečně provázány informace o uživateli, např. Osobní data 7 nebo přístupová práva, s elektronickou identitou uživatele a to tak, že prostředky Poskytovatele služeb 5, resp. Terminálu 9, mají přímo k dispozici příslušné informace v kontextu Obslužného programu služby 6, resp. Obslužného programu terminálu 19.

V průběhu užívání služby může dojít na základě součinnosti PEIG-M 3 a PEIG-P 8 k přidání další elektronické identity, ke změně identifikátorů, k zrušení elektronické identity nebo k dalším změnám. V návaznosti na elektronickou identitu mohou být nastavována přístupová práva a další uživatelské atributy služby.

Součinnost PEIG-M 3 a PEIG-P 8 může podporovat i další činnosti spojené s elektronickou identitou. Může jít o podporu bezpečného předávání informací, např. osobních dat mezi různými poskytovateli služeb při zachování důvěrnosti elektronické identity uživatele nebo o specielní činnosti spojené s podporou transakcí mezi uživatelem a více poskytovateli služeb, jako jsou např. elektronické platby.

Při vzájemné součinnosti PEIG-M 3 a PEIG-P 8 jsou využívány následující postupy a prostředky:

- **PEIG 1 (Personal Electronic Identity Gadget – osobní nosič elektronické identity)** – Jedná se o automatizované speciální zařízení nebo část zařízení univerzálně využívané svým vlastníkem-uživatelem pro všechny činnosti spojené s elektronickou identitou. Zařízení je určeno k osobnímu používání jednou osobou. Jedná se o malé snadno přenosné zařízení umožňující vlastníkovi uživateli nosit svoji elektronickou identitu stále s sebou. Významnou vlastností zařízení je jeho extrémně jednoduché používání.

  Vlastnictví-užívání PEIG 1 je dobrovolné a jedna osoba-uživatel smí vlastnit a užívat i více PEIG 1.

  Aktivace PEIG 1 je oddělena od elektronické identity. Data užívaná pro aktivaci PEIG 1 nejsou používána pro elektronickou identitu a naopak, data užívaná pro elektronickou identitu nejsou užívána k aktivaci PEIG 1.

  PEIG 1 je sám o sobě nerozlišitelný od jiných PEIG 1. Je vyráběn prázdný, bez jakékoli elektronické identity a bez informací potřebných k personifikované aktivaci PEIG 1 .

- **Nezávislý, anonymní a časově proměnný identifikátor** - PEIG-M 3 a PEIG-P 8 užívají pro odlišení uživatelů identifikátory.

  Tyto identifikátory jsou nezávislé, to znamená, že pro jednoho uživatele jeden PEIG-M 3 užívá různé identifikátory pro různé Poskytovatele služeb 5. Ovšem tím, že jeden Poskytovatel služeb 5 zná identifikátor uživatele jen pro své služby, nemůže zjistit, zda příslušný uživatel používá služby také jiného Poskytovatele služeb 5, ani jaké služby a jak je používá. Tím je chráněn uživatel před neoprávněným shromažďováním informací o svém chování.

  Tyto identifikátory jsou anonymní, to znamená, že identifikátor neobsahuje žádnou informaci, pomocí které je možné přímo či nepřímo zjistit totožnost uživatele. Neobsahuje ani jméno, ani části jména, ani rodné číslo či jiné údaje, pomocí kterých lze určit či odhadnout, která fyzická osoba identifikátor používá.

  Tyto identifikátory jsou časově proměnné, to znamená, že identifikátor platí jen po omezenou dobu. Před uplynutím doby platnosti může být identifikátor nahrazen jiným identifikátorem bez ztráty identity a personifikovaného kontextu.

- **Symetrická identita** – vytváření identifikátoru a ověřování identity je symetrické. Činnosti PEIG-M 3 a PEIG-P 8 jsou vyvážené. Žádná strana nemá dominantní postavení, ani jedna strana nemůže bez spolupráce druhé strany vytvořit nebo ověřit identitu.

  PEIG-M 3 vytvoří svoji část identifikátoru a PEIG-P 8 také svoji část identifikátoru. Identifikátor vznikne kombinací obou částí.

  PEIG-P 8 ověřuje identitu na straně uživatele pomocí tajné informace spojené s identitou předávanou PEIG-M 3 a naopak PEIG-M 3 ověřuje identitu na straně Poskytovatele služeb 5 pomocí tajné informace spojené s identitou předávanou PEIG-P 8. Teprve po úspěšném ověření obou stran je identita považována za ověřenou.

- **Jednorázový sdílený identifikátor** – slouží k důvěryhodnému propojení informací jediné transakce mezi více poskytovateli služeb 5 bez narušení nezávislosti identifikátorů používaných jedním vlastníkem-uživatelem PEIG 1 s více Poskytovateli služeb 5.

  Identifikátor je vygenerován jen pro účel jediné transakce zajištěného přenosu informací mezi Poskytovateli služeb 5 a je důvěryhodně propojen s informacemi, které mají být předány v rámci transakce a zároveň s identifikátory užívanými jednotlivými Poskytovateli služeb 5 a to tak, že každý Poskytovatel služeb 5 má k dispozici pouze takové informace, které mu přísluší a zároveň má důvěryhodně zajištěno, že předávané informace se týkají příslušného uživatele-vlastníka PEIG 1.

- **Oddělení osobních informací** – veškeré osobní informace a další informace týkající se osoby uživatele jsou odděleny od elektronické identity. Tyto osobní informace nejsou obsaženy v komunikaci mezi PEIG-M 3 a PEIG-P 8 ani v obsahu PEIG 1. Personální informace mohou být uloženy odděleně v systému Poskytovatele služeb 5 a důvěryhodně provázány s elektronickou identitou. Poskytovatel služby 5 má k dispozici jen takové osobní údaje, které mu uživatel předal, nebo takové osobní údaje, které mu předal jiný Poskytovatel služeb 5 na základě uživatelova souhlasu. Zároveň může Poskytovatel služeb 5 osobní údaje o uživatelích efektivně chránit ve svých vnitřních systémech, protože tato data ani jejich části či odvozené údaje nejsou používány při zjišťování a ověřování elektronické identity.

- **Asymetrická kryptografie bez osobních dat** – technologie asymetrické kryptografie je používána bez jakýchkoli osobních údajů. Jsou používány standardní páry klíčů veřejný a privátní jako v běžné PKI (Public Key Infrastructure), ale nejsou používány žádné datové struktury obsahující osobní údaje, například certifikáty. Nejsou používány ani postupy a činnosti spojené s těmito osobními údaji, například certifikační politiky, ověřování fyzické identity apod.

- **Shluk identit (Identity Cluster)** – jeden Poskytovatel služeb 5 může propojit více svých technických služeb s jedinou identitou uživatele. Všechny takto propojené služby budou užívat tentýž identifikátor uživatele. Takové propojení může Poskytovatel služeb 5 použít k různým účelům, například k tomu, aby důvěryhodně propojil osobní data o uživateli zajišťovaná jednou technickou službou se službami poskytovanými uživateli pomocí jiné technické služby. Takové propojení bude řízeno a kontrolováno systémem řízení bezpečnosti jednoho Poskytovatele služeb 5.

- **Samodestrukční mechanismus** – v případě nesprávné nebo neúspěšné aktivace PEIG 1 neoprávněnou osobou může být automaticky aktivován samodestrukční mechanizmus, který místo toho, aby zpřístupnil služby neoprávněné osobě, zruší platnost identifikace a to jak obsažené v PEIG-M 3 na straně uživatele, tak v PEIG-P 8 na straně Poskytovatele služeb 5. Identifikátory a funkční možnosti PEIG-M 3 a PEIG-P 8 jsou připraveny k takové destrukci buď na základě nesprávné aktivace PEIG-M 3 a/nebo na základě omezeného času platnosti identifikátoru. K destrukci identifikátorů na základě omezené platnosti dojde i v případě, že PEIG 1 není delší dobu používán, například při jeho ztrátě.

- **Bezpečnostní úrovně** – úroveň zabezpečení elektronické identity je popsána pomocí technologicky neutrálních a nezávisle ověřitelných bezpečnostních úrovní. Každý uživatel a každý poskytovatel služby 5 může jednoduše zjistit, jaké bezpečnostní úrovni odpovídá příslušný produkt, a tedy jaké bezpečnostní parametry naplňuje či jakým bezpečnostním nárokům vyhovuje.

- **Oddělení síťové komunikace** – jednotlivé moduly elektronické identity PEIG-M a PEIG-P spolu vzdáleně nekomunikují přímo. Vlastní komunikace po Rozsáhlé síti 11 je oddělena pomocí specializovaných síťových bezpečnostních prvků, a to jak na straně Poskytovatele služeb 5 (Firewall 12), tak na straně uživatele (Proxy 15). PEIG 1 může fyzicky komunikovat jen na velmi malou vzdálenost a to pomocí jiných

prostředků komunikace (Lokální komunikační kanál **16**), než které používá ke komunikaci se vzdáleným Poskytovatelem služeb **5** (Vzdálený komunikační kanál **14**).

Průmyslová využitelnost

Vlastní komunikace mezi PEIG-M **3** a PEIG-P **8**, resp. PEIG-P terminálu **20**, na úrovni Logického komunikačního kanálu **17**, resp. Lokálního logického komunikačního kanálu **20**, je popsána potřebnými pravidly, která umožňují standardizaci a vzájemnou spolupráci produktů různých výrobců. Způsob, jakým jsou pravidla vytvořena a popsána, umožňuje využití běžných prostředků k realizaci Logického komunikačního kanálu **17** a tím i využití existujících technologií a prostředků pro účely elektronické identity.

Příslušné komunikační kanály, Vzdálený komunikační kanál **14** a Lokální komunikační kanál **16**, jsou také popsány v popisu rozhraní elektronické identity a to v různých variantách. Logický komunikační kanál **17**, resp. Lokální logický komunikační kanál **20**, tak může být realizován pomocí různých variant komunikačních kanálů. V budoucnu může dojít k využití jiných dnes neznámých či nepoužívaných komunikačních kanálů.

V rámci rozšiřitelné funkčnosti jsou jednotlivé moduly elektronické identity PEIG-M **3** a PEIG-P **8** konstruovány jako virtuální specializované počítače s rozšiřitelnou instrukční sadou. To umožní budoucí rozšiřování o nově potřebné činnosti spojené s novými požadavky nebo dalšími oblastmi použití, například nové funkčnosti pro podporu elektronických plateb.

PATENTOVÉ NÁROKY

1. Způsob navazování chráněné elektronické komunikace mezi různými elektronickými prostředky, zejména mezi elektronickými prostředky poskytovatelů elektronických služeb a elektronickými prostředky uživatelů elektronických služeb a/nebo mezi lokálními elektronickými prostředky a elektronickými prostředky uživatelů elektronických služeb, **vyznačující se tím**, že se uživatelé elektronických služeb nejprve vybaví osobním nosičem elektronické identity bez informací o identitě uživatele, načež až při prvním připojení prázdného osobního nosiče uživatele na elektronické prostředky libovolného poskytovatele služeb a/nebo na lokální elektronické prostředky, si osobní nosič elektronické identity a elektronické prostředky poskytovatele služeb a/nebo lokální elektronické prostředky vzájemně vygenerují ověřitelnou elektronickou identitu, která se v osobním nosiči elektronické identity a v elektronických prostředcích poskytovatele služeb a/nebo v lokálních elektronických prostředcích uloží pro potřeby další vzájemné elektronické komunikace, odděleně od ostatních identit a bez znalostí osobních údajů o uživateli elektronických služeb, přičemž následně se jen vygenerované a uložené informace využijí k ověření identity při každém dalším připojení uživatele elektronických služeb na elektronické prostředky toho kterého poskytovatele služeb a/nebo na lokální elektronické prostředky.

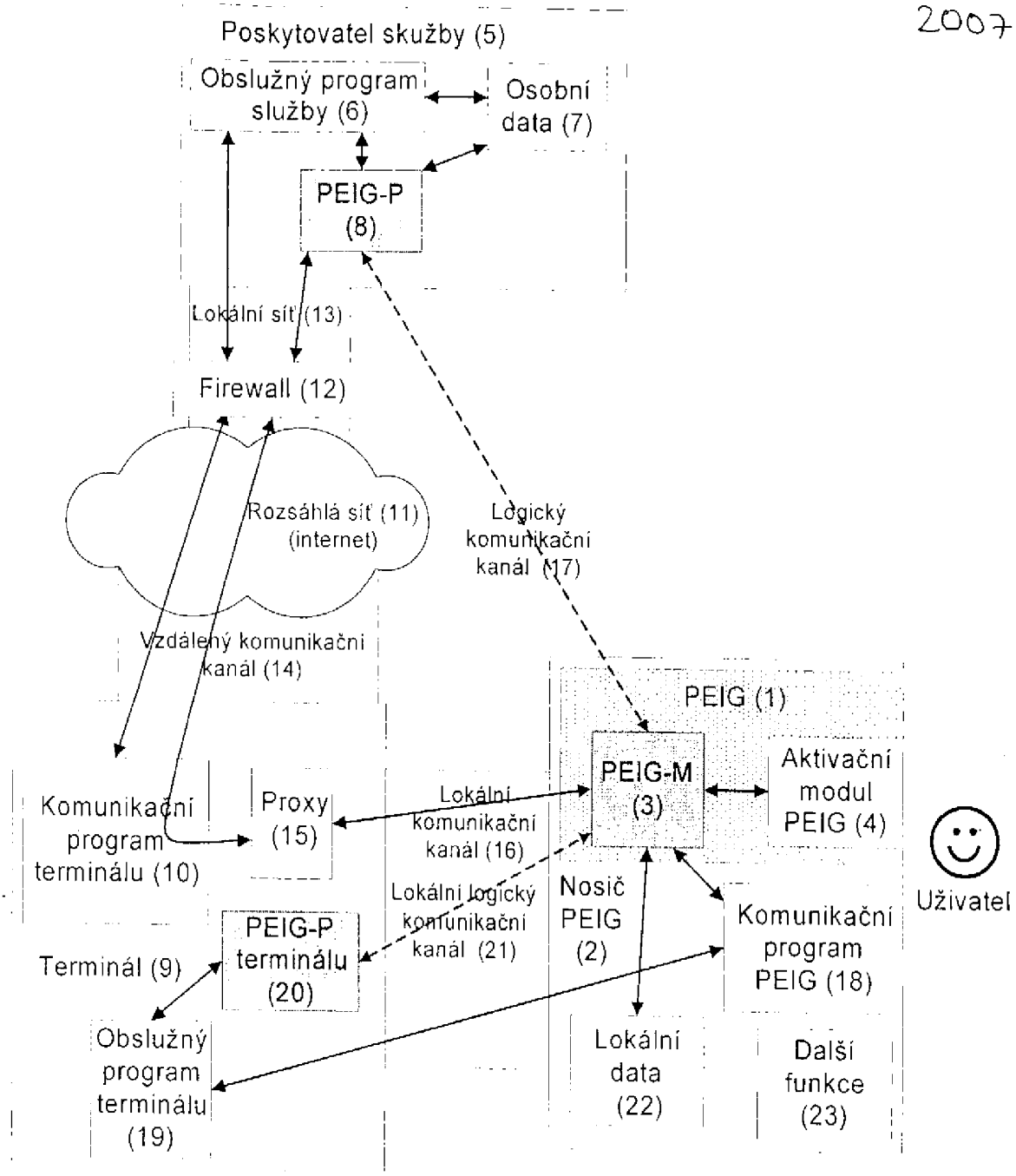
2. Způsob podle nároku 1, **vyznačující se tím**, že se uložené informace využijí k ověření identity při každém dalším připojení uživatele elektronických služeb na elektronické prostředky tohoto poskytovatele služeb a/nebo na lokální elektronické prostředky před každou změnou ověřitelné elektronické identity, při které je identifikátor nahrazen jiným identifikátorem bez ztráty identity a personifikovaného kontextu.

3. Způsob podle nároku 1, **vyznačující se tím**, že po poskytnutí osobních údajů elektronickým prostředkům poskytovatele služeb a/nebo lokálnímu elektronickému prostředku a souhlasu uživatele služeb s jejich předáním alespoň elektronickým prostředkům jednoho dalšího poskytovatele služeb a/nebo lokálnímu elektronickému prostředku se osobním nosičem elektronické identity spolu s elektronickými prostředky zúčastněných poskytovatelů služeb a/nebo spolu s lokálními elektronickými prostředky vygeneruje přechodná jednoúčelová elektronická identita určená k realizaci předání osobních dat uživatele mezi zúčastněnými poskytovateli služeb a/nebo lokálními elektronickými prostředky.

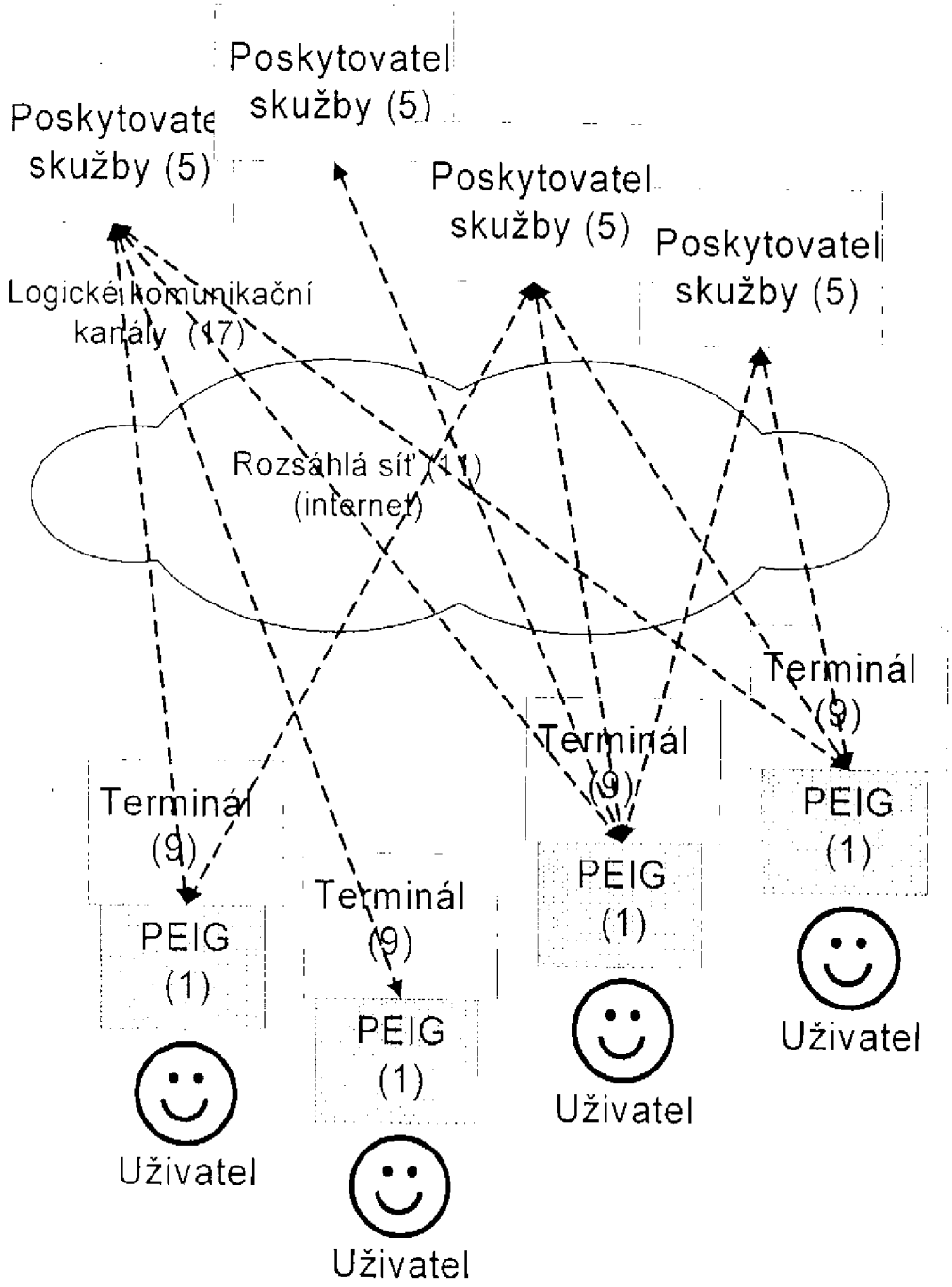
4. Způsob podle nároku 1, **vyznačující se tím**, že se vytváření ověřitelné elektronické identity a ověřování identity provádí symetricky tak, že kombinací jedné části identifikátoru generovanou osobním nosičem elektronické identity a druhé části identifikátoru generovanou elektronickými prostředky poskytovatelů elektronických služeb nebo lokálními elektronickými prostředky vznikne identifikátor, který ani jedna strana nemůže bez spolupráce druhé strany vytvořit nebo ověřit, přičemž osobní nosič elektronické identity ověřuje identitu na straně uživatele pomocí tajné informace spojené s identitou, předávané elektronickými prostředky poskytovatelů elektronických služeb nebo lokálními elektronickými prostředky, a naopak elektronické prostředky poskytovatelů elektronických služeb nebo lokální elektronické prostředky ověřují identitu na straně poskytovatele služeb nebo na straně lokálního elektronického prostředku, pomocí tajné informace spojené s identitou, předávané osobním nosičem elektronické identity, načež teprve po úspěšném ověření identifikátorů obou stran je identita považována za ověřenou.

5. Způsob podle nároku 1, **vyznačující se tím**, že provádění asymetrické kryptografie se standardními páry klíčů se uskutečňuje s vypuštěním všech datových struktur obsahujících osobní údaje a s vypuštěním postupů a činností spojených s těmito osobními údaji.

6. Způsob podle nároku 1, **vyznačující se tím**, že se nesprávnou nebo neúspěšnou aktivací osobního nosiče elektronické identity může spustit samodestrukční mechanizmus pro zrušení platnosti identifikace obsažené v osobním nosiči elektronické identity jak na straně uživatele, tak v elektronických prostředcích poskytovatelů elektronických služeb a/nebo lokálních elektronických prostředcích na straně poskytovatele služeb a/nebo lokálních elektronických prostředků.



Obr.1



Obr.2