PŘIHLÁŠKA VYNÁLEZU

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

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(22) Přihlášeno: **16.03.2007**

(40) Datum zveřejnění přihlášky vynálezu **24.09.2008**

(Věstník č. 39/2008)

(21) Číslo dokumentu:

2007-205

(13) Druh dokumentu: **A3**

(51) Int. Cl.:

H04L 9/32	(2006.01)
G06Q 20/00	(2006.01)
G06Q 40/00	(2006.01)
G06F 19/00	(2006.01)
G07F 7/00	(2006.01)

(71) Přihlašovatel:

MONET+, a. s., Zlín - Štípa, CZ

(72) Původce:

Endrys Břetislav Ing., Zlín, CZ

(74) Zástupce:

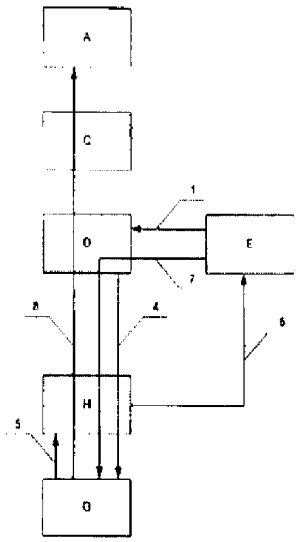
ROTT, RŮŽIČKA & GUTTMANN Patentová, známková a advokátní kancelář, Ing. Ivana Jirotková, Nad Štolou 12, Praha 7, 17000

(54) Název přihlášky vynálezu:

Způsob vytváření autorizovaného elektronického podpisu oprávněné osoby a zařízení k provádění tohoto způsobu

(57) Anotace:

Vynález řeší posílení důvěryhodnosti elektronického podpisu dat vložením dalšího kontrolního mechanismu s aktivní interakcí oprávněné osoby (E), který odhalí případný útok na podepisovaná data. Způsob vytváření autorizovaného elektronického podpisu oprávněné osoby (E), spočívá v tom, že podepisovaná data, která mají být opatřena elektronickým podpisem se zadají do řídicího systému (D), načež se uloží do vnitřní paměti tokenu (G), jehož držitelem je oprávněná osoba (E). Podepisovaná data se do tokenu (G) uloží v kompletní podobě a/nebo v podobě kryptografického otisku, načež před realizací elektronického podpisu se vygeneruje externě, to je vně tokenu G, nebo v tokenu G dodatečný jednorázový autorizační kód JAK, patřící k podepisovaným datům. Podepisovaná data se společně s jednorázovým autorizačním kódem JAK sdělí prostřednictvím samostatného, nezávislého informačního zařízení, jež není součástí řídicího systému (D), oprávněné osobě (E), která provede jejich kontrolu, poté se jednorázový autorizační kód JAK, s výhodou spolu s dalšími ochrannými prvky, zadají do tokenu (G), kde se použijí jako přístupová podmínka pro získání hodnoty elektronického podpisu, přičemž v tokenu (G) se provede kontrola, zda jednorázový autorizační kód JAK, a další ochranné prvky, byly zadány správně, přičemž v kladném případě token (G) vytvoří hodnotu elektronického podpisu, která se odešle s daty do subjektu (A), pro nějž je autorizovaný elektronický podpis vytvářen, zejména do banky nebo jiného subjektu.



CZ 2007 - 205 A3

Způsob vytváření autorizovaného elektronického podpisu oprávněné osoby a zařízení k provádění tohoto způsobu

Oblast techniky

Vynález se týká způsobu vytváření autorizovaného elektronického podpisu oprávněné osoby a dále se týká zařízení pro provádění tohoto způsobu.

Dosavadní stav techniky

Současný stav techniky nepopisuje metody implementované uvnitř tokenu, které by vynutily kontrolu podepisovaných dat uživatelem, který se data chystá podepsat. Existují přitom situace, kdy je tato kontrola velmi důležitá, například v systémech, které jsou schopny realizovat elektronické transakce vysoké hodnoty. V současné době totiž nelze spoléhat na bezpečnost osobních počítačů a aplikací, které jsou na těchto osobních počítačích spouštěny. Komplikované a rozsáhlé funkce programového vybavení osobních počítačů, například operační systém, aplikace pro přístup na internet, další aplikace atd., vytvářejí podmínky pro snadné a těžce detekovatelné spouštění aplikací, které nejsou pod výhradní kontrolou uživatele osobního počítače a které mohou v některých případech vykonávat činnosti směřující k poškození nejen samotného uživatele osobního počítače, ale i jiných subjektů.

Podstata vynálezu

Uvedené nevýhody odstraňuje způsob vytváření autorizovaného elektronického podpisu oprávněné osoby a zařízení k provádění tohoto způsobu podle předloženého vynálezu. Předkládané řešení využívá bezpečnostních vlastností tokenů. Token je schopen bránit sám sebe před vnějšími útoky a navíc umožňuje bezpečné vykonávání operací, kryptografických i nekryptografických. Může tedy aktivně podpořit funkce související s kontrolou elektronicky podepisovaných dat, ještě před jejich podepsáním.

Při provádění způsobu vytváření autorizovaného elektronického podpisu dat oprávněnou osobou se data, která mají být opatřena elektronickým podpisem, zadají do řídícího systému. Podstata způsobu spočívá v tom, že podepisovaná data se uloží do vnitřní paměti tokenu, jehož držitelem je oprávněná osoba v kompletní podobě a/nebo v podobě kryptografického

otisku. Před realizací elektronického podpisu se vygeneruje dodatečný jednorázový autorizační kód, patřící k podepisovaným datům a podepisovaná data se společně s jednorázovým autorizačním kódem sdělí prostřednictvím samostatného, nezávislého informačního zařízení, jež není součástí řídícího systému, oprávněné osobě, aby tato provedla jejich kontrolu. Poté se jednorázový autorizační kód spolu s dalšími ochrannými prvky zadají do tokenu, kde se použijí jako přístupová podmínka pro vytvoření elektronického podpisu a vrácení jeho hodnoty, tj. v tokenu se provede kontrola, zda jednorázový autorizační kód, případně další ochranné prvky, byly zadány správně. V kladném případě token vytvoří a řídícímu systému poskytne hodnotu elektronického podpisu, která se odešle s daty do subjektu, pro nějž je autorizovaný elektronický podpis vytvářen, zejména do bankovní aplikace nebo jiného nezávislého a věrohodného subjektu. Výhodou tohoto způsobu je zvýšení principu neodmítnutelnosti odpovědnosti za elektronická data – oprávněná osoba, která je na řídícím systému nezávislým zařízením informována o tom, co podepisuje, musí stvrdit souhlas s podpisem dodatečným jednorázovým autorizačním kódem, který je dočasně platný pouze pro právě podepisovaná data. Díky nezávislosti informačního zařízení na řídícím systému je značně ztížen potencionální útok – případný útočník není schopen zjistit hodnotu jednorázového autorizačního kódu a tím pádem není schopen vykonat operaci elektronického podpisu, o níž by oprávněná osoba nevěděla. Podepisující oprávněná osoba, to je původce dat, přesně ví co podepisuje a příjemce, to je konzument dat, má definovanou úroveň jistoty o identitě původce zprávy.

Při výhodném provádění způsobu se jednorázový autorizační kód vygeneruje v tokenu před realizací elektronického podpisu a sdělí se oprávněné osobě spolu s podepisovanými daty prostřednictvím samostatného, nezávislého informačního zařízení, kterým je s výhodou čtecí zařízení, přičemž se blokuje přenos jednorázového autorizačního kódu z tokenu do řídícího systému. Výhodou je zde to, že se celá operace vykoná lokálně bez dodatečných nároků na komunikační infrastrukturu a dále bez nutnosti budování dalších komponent centrálního systému. Z pohledu strany, která je závislá na elektronickém podpisu se v tomto případě nemění logistika zpracování podepsaných dat, případně se nemění komponenty pokud jsou v systému implementovány, které se podílí na přípravě dat určených k autorizaci elektronickým podpisem.

Jiná výhodná varianta způsobu se vyznačuje tím, že jednorázový autorizační kód se vygeneruje před realiazací elektronického podpisu subjektem, pro nějž je autorizovaný

elektronický podpis vytvářen. nebo jiným, nezávislým a věrohodným systémem. Subjekt, nebo jiný, nezávislý a věrohodný systém, který jednorázový autorizační kód generuje, zapíše jednorázový autorizační kód spolu s daty určenými pro podpis do tokenu tak, že neautorizovaný subjekt nemůže hodnotu jednorázového autorizačního kód získat ani modifikovat a nemůže modifikovat data určená k podpisu, případně jejich kryptografický otisk. Mezi tokenem a subjektem či jiným, nezávislým a věrohodným systémem, který generuje jednorázový autorizační kód je tedy sdíleno společné tajemství používané pro ustavení tohoto kryptografického kanálu. Dále se jednorázový autorizační kód sdělí oprávněné osobě společně s podepisovanými daty prostřednictvím samostatného, nezávislého informačního zařízení, které není ovlivnitelné řídícím systémem, s výhodou tak, že se zobrazí na displeji zařízení, kterým je výhodně mobilní telefon oprávněné osoby.
Výhodou je zde to, že lze s využitím stávající infrastruktury a s existujícími zařízeními poměrně rychle vybudovat systém tvorby autorizovaného elektronického podpisu. Nezanedbatelnou výhodou je i to, že oprávněná osoba používá zařízení, které zná a nemusí se učit ovládání nového zařízení.

Výhodně lze bezpečnost provádění způsobu posílit tak, že se jednorázový autorizační kód vygeneruje v rámci dočasného sezení, ve kterém je token schopen podepsat data, z čehož plyne, že tento kód je použitelný pouze pro autorizaci podpisu dat, která byla do tokenu v rámci tohoto sezení poslána, to je platnost jednorázového autorizačního kódu je ukončena například odpojením napájení tokenu, resetováním tokenu, inicializací nového sezení pro vytvoření elektronického podpisu atp.
Výhodou je zde to, že lze definovaným způsobem předčasně ukončit platnost jednorázového autorizačního kódu a tím v případě potřeby zabránit vytvoření elektronického podpisu dat.

S výhodou je způsob prováděn tak, že se operace vytvoření elektronického podpisu konkrétních dat zablokuje, případně se zabrání poskytnutí hodnoty elektronického podpisu, pokud se po provedení kontroly v tokenu zjistí překročení povoleného počtu nesprávného zadání jednorázového autorizačního kódu, či dalších ochranných prvků.
Výhodou je zde to, že token sám dokáže zabránit získání hodnoty elektronického podpisu při podezření na útok, při němž se případný útočník snaží uhodnout hodnotu jednorázového autorizačního kódu či jiných ochranných prvků.

Zařízení pro provádění způsobu podle vynálezu ve výhodném provedení má řídící systém propojen se subjektem, pro nějž je elektronický podpis vytvářen, pomocí první komunikační infrastruktury. Dále je řídící systém obousměrně propojen se samostatným na řídícím systému, nezávislým informačním zařízením, kterým je s výhodou nezávislé čtecí zařízení, jež je obousměrně propojeno s tokenem, a je upraveno pro přenos dat mezi řídícím systémem a tokenem a pro předání vybraných přenášených dat oprávněné osobě, která je držitelem tokenu. Toto, nezávislé informační zařízení je upraveno pro zabránění přenosu vybraných citlivých dat z tokenu do řídícího systému.

Další výhodná varianta zařízení pro provádění způsobu je vytvořena tak, že řídící systém je přes první komunikační infrastrukturu propojen se subjektem, pro nějž je vytvářen elektronický podpis, přičemž tento subjekt je propojen jednak přes druhou komunikační infrastrukturu, nezávislou na první komunikační infrastruktuře sítě, se samostatným informačním zařízením pro předání jednorázového autorizovaného kódu a podepisovaných dat oprávněné osobě, která je držitelem tokenu a jednak přes první komunikační infrastrukturu a řídící systém propojen s tokenem.

Další výhodná varianta zařízení pro provádění způsobu je vytvořena tak, že řídící systém je přes první komunikační infrastrukturu propojen se subjektem, pro nějž je vytvářen elektronický podpis a s na subjektu nezávislým a věrohodným systémem pro generování a/nebo zašifrování jednorázového autorizačního kódu a s výhodou opatření dalších ochranných prvků k podepisovaným datům pro token, přičemž nezávislý a věrohodný systém je propojen přes druhou komunikační infrastrukturu nezávislou na první infrastruktuře sítě, se samostatným informačním zařízením pro předání jednorázového autorizovaného kódu a podepisovaných dat oprávněné osobě, která je držitelem tokenu.

Výhodně může být nezávislý a věrohodný systémem pro generování a/nebo zašifrování jednorázového autorizačního kódu a opatření ochranných prvků k podepisovaným datům pro token buď součástí subjektu, pro který jsou podepisovaná data vytvářena, případně může být nezávislým, ale důvěryhodným systémem, který své služby poskytuje více nezávislým subjektům, pro které jsou vytvářeny elektronické podpisy dat. Výhodou je zde úspora nákladů na budování a provoz tohoto systému, kdy se více subjektů na těchto nákladech spolupodílí.

Jako první komunikační infrastruktura je s výhodou použita internetová síť.

Druhou komunikační infrastrukturou může být s výhodou GSM síť.

Zařízení s výhodou používá jako řídicí systém osobní počítač.

Funkce tokenu jsou s výhodou implementovány v čipové kartě.

Funkce tokenu jsou s výhodou implementovány společně v tradiční, čipové kartě, nebo podobném tradičním zařízení a v dodatečném nezávislém pomocném zařízení. Výhodou je zde to, že dosud používané čipové karty bez integrované podpory vynucení dodatečné autorizace jednorázovým kódem mohou být využity pro tvorbu autorizovaného elektronického podpisu s využitím jednorázového autorizačního kódu tak, jak je to popsáno v tomto vynálezu. Chybějící funkcionality generování a ověřování jednorázového autorizačního kódu jsou implementovány v dodatečném nezávislém pomocném zařízení, které spolu s čipovou kartou tvoří token, tak jak je popisován v tomto vynálezu.

Přehled obrázků na výkresech

Podstata vynálezu je zřejmá z přiložených obrázků.

Na obr. 1 a 2 jsou zobrazeno zařízení a jsou označeny jednotlivé kroky způsobu k autorizovanému vytvoření elektronického podpisu s využitím varianty, kdy je jednorázový autorizační kód JAK generován vně tokenu. Pro zobrazení hodnoty JAK kódu i obsahu podepisovaných dat je použito nezávislého kanálu například ve formě GSM sítě, služeb operátora a mobilního telefonu. Varianta dle obr.1 ukazuje případ, kdy subjekt, pro nějž jsou vytvářena podepisovaná data sám komunikuje s podepisující osobou i tokenem, zatímco varianta dle obr.2 ukazuje případ, kdy v systému existuje na subjektu, pro nějž jsou vytvářena podepisovaná data jiný, nezávislý důvěryhodný subjekt, který zajišťuje důvěryhodnou komunikaci s oprávněnou osobou , to je s podepisující osobou i tokenem.

Na obr. 3 je zobrazeno zařízení a kroky způsobu autorizovaného vytvoření elektronického podpisu s využitím varianty, kdy je kód JAK generován uvnitř tokenu. Pro zobrazení hodnoty JAK kódu i obsahu podepisovaných dat je použito speciálního čtecího zařízení vybaveného zobrazovačem. Obr. 4 zobrazuje token vytvořený z nezávislého pomocného zařízení a

tradičního zařízení pro tvorbu elektronického podpisu, představovaného například tradiční čipovou kartou.

Příklady provedení vynálezu

Příkladným provedením vynálezu je implementace systému pro bezpečné zadávání elektronických platebních příkazů prostřednictvím webového rozhraní aplikace s použitím:

běžného osobního počítače jako řídicího systému D pro komunikaci s webovou aplikací banky, resp subjektu A a prostřednictvím internetového prohlížeče a dalších přídavných SW a HW realizující funkce autentizace, zejména však zadávání a podepsání vlastního platebního příkazu,

tokenu G s výše popisovanými vlastnostmi, které umožňují autorizované vytvoření elektronického podpisu,

výhodně

samostatného informačního zařízení F , například mobilního telefonu a sítě GSM, jejichž prostřednictvím je oprávněné osobě E,

resp.klientovi banky, zasílán kód JAK spolu s obsahem podepisované transakce, viz schéma dle obr. 1 a 2,

speciálního čtecího zařízení H, které sleduje a případně modifikuje komunikaci mezi osobním počítačem a tokenem G, přičemž je schopno zobrazit důležité informace například hodnotu JAK kódu a příslušných podepisovaných dat a dále je schopno zabránit přenesení hodnoty JAK kódu z tokenu G, resp čipové karty do řídicího systému D, resp. osobního počítače, viz schéma dle obr. 3.

Varianta způsobu prováděná zařízením dle obr.1 spočívá v externím generování hodnoty jednorázového autorizačního kódu JAK, to je, vně tokenu G, s použitím první komunikační infrastruktury C, kterou je internetová síť a s využitím druhé komunikační infrastruktury B, kterou je GSM síť, jako nezávislého kanálu pro zobrazení podepisovaných dat a příslušné hodnoty jednorázového autorizačního kódu JAK.

V prvém kroku 1, oprávněná osoba E, v tomto, případě klient subjektu A, resp. banky, zadá prostřednictvím formuláře na řídicím systému D, kterým je zde osobní počítač, data elektronické transakce, která má být vykonána bankou. Tato data jsou přenesena první komunikační infrastrukturou C, kterou je internetová síť, do prostředí subjektu A, resp. do banky. V druhém kroku 2 je subjektem A, resp. bankou, vygenerována k datům elektronické transakce náhodná hodnota jednorázového autorizačního kódu JAK. Hodnota JAK kódu

sestává např. ze čtyř číslic. Dále banka vytvoří hash dat, která mají být podepsána a zajistí jejich odeslání a šifrovaný zápis do tokenu G.

Šifrovaný zápis dat do tokenu G může představovat několik dílčích kroků:

a) zapnutí napájení tokenu G,
b) výběr PKI aplikace,
c) požadavek na token G na vygenerování bloku dat, která budou použita pro ustavení šifrovaného kanálu,
d) v bezpečném prostředí banky je na základě dat získaných z předchozího bodu vygenerován šifrovací klíč (algoritmus alespoň 3DES, lépe AES, algoritmus výměny klíčů může být proprietární, popř. může být použit některá ze standardizovaných metod, jako např. Diffie-Hellman key agreement).
e) pomocí vygenerovaného šifrovacího klíče je sestaven blok dat pro token G, přičemž blok dat obsahuje
    i. s výhodou doplňující informace, pomocí nichž token G odvodí použitý šifrovací klíč,
    ii. s výhodou zašifrovanou informaci o maximálním počtu opakování pokusů zadání hodnoty JAK kódu oprávněnou osobou E ,obvykle budou povolena 3 neúspěšná zadání,
    iii. zašifrovanou hodnotu JAK kódu,
    iv. šifrovanou nebo alespoň podepsanou hodnotu hash podepisovaných dat, s výhodou elektronický podpis všech nebo vybraných částí bloku dat posílaných do tokenu G, který ověřením podpisu zjistí, zda byla data generována důvěryhodným systémem,
f) blok dat dle předchozího bodu je přenesen na tokenu G, kde je zpracován, to je, je ustaven šifrovací klíč a jsou provedeny syntaktické a kryptografické kontroly.

V následujícím třetím kroku 3 banka odešle hodnotu vygenerovaného JAK kódu, spolu se všemi důležitými náležitostmi elektronické transakce, kterou oprávněná osoba E zadala v prvém kroku, např. typ transakce, cílový účet, částku, variabilní symbol, atd. prostřednictvím druhé komunikační infrastruktury B, například GSM sítí, SMS zprávou na mobilní číslo oprávněné osoby E. Konkrétní číslo mobilního telefonu oprávněné osoby E je drženo v interní databázi banky. Zde je velmi důležité, aby komunikace s GSM operátorem byla dostatečně zabezpečena tak, aby nemohla být zneužita potenciálním útočníkem.

V dalším, kroku 6, oprávněná osoba E, resp. klient banky, současně držitel samostatného informačního zařízení F, například mobilního telefonu a tokenu G, zkontroluje náležitosti

transakce, zejména shodu s parametry transakce, které zadal v prvém kroku. Současně si přečte hodnotu JAK kódu. Pokud se náležitosti platby shodují s parametry transakce, klient banky pokračuje následujícím krokem 7. Pokud klient banky nehodlá transakci potvrdit svým podpisem, přeruší celý proces.

V následujícím kroku 7 klient banky zadáním PIN se přihlásí na token G a zadáním JAK kódu, to je potvrzením parametrů transakce, tokenu G, potvrdí provedení transakce. Nutno připomenout, že token G je před-inicializován z kroku 2. Token G provede kontrolu PIN, pokud není zadán správně, pak obslužný řídící kód k tokenu umožní opakované zadání PIN tak dlouho, dokud není zablokován. Podobně token G provádí kontrolu JAK kódu – dokud není dosaženo maximálního počtu opakovaného zadání chybné hodnoty JAK kódu, obvykle 3 pokusy, je umožněno znovuzadání JAK kódu. Pokud je některý z ověřovacích kódů - PIN, JAK - zablokován nebo je token G resetován či odpojen od zdroje napájení, není možné operaci dokončit. Pokud jsou všechny přístupové podmínky správně ověřeny, pokračuje se krokem 8.

Protože token G úspěšně provedl veškeré kontroly přístupových podmínek, je v rámci kroku 8 v tokenu G vypočítána hodnota elektronického podpisu dat, jejichž kryptografický otisk byl zapsán do paměti tokenu G v kroku 2. Hodnota elektronického podpisu je odeslána do banky, kde je dále zpracovávána běžnými postupy.

Výhodou této varianty je to, že pro realizaci funkce vytvoření autorizovaného elektronického kódu využívá dvě nezávislé existující komunikační infrastruktury a to první komunikační infrastrukturu C, kterou je internetová síť, pro komunikaci mezi subjektem A, resp. bankou, na jedné straně a oprávněnou osobou E, řídícím systémem D, to je osobním počítačem a tokenem G na straně druhé. První komunikační infrastruktura C zprostředkovává přenos dat k podepsání, přenos šifrovaného JAK kódu svázaného s konkrétní transakcí a přenos vlastního podpisu dat. Druhou komunikační infrastrukturou B je sít GSM operátora pro zasílání informačních zpráv, doplněných o externě generovaný jednorázový kód JAK, který je oprávněnou osobou E přenesen do tokenu G, například čipové karty, kde je porovnán s jednorázovým JAK kódem, který před tím byl do čipové karty šifrovaně zapsán.

Další varianta způsobu je prováděna zařízením dle obr.2, kdy se opět provádí externí generování hodnoty JAK kódu s použitím GSM sítě jako nezávislého kanálu pro zobrazení podepisovaných dat a příslušné hodnoty JAK kódu s využitím důvěryhodného, nezávislého systému I pro rozesílání SMS zpráv a šifrovanou komunikaci s tokenem G.

V tomto případě se jedná o modifikaci předchozího případu s tím, že kroky 2 a 3 neprovádí subjekt A, resp. banka, ale jsou prováděny nezávislým důvěryhodným subjektem I.

V kroku 1 způsobu oprávněná osoba E, klient banky zadá prostřednictvím formuláře na řídícím systému D, resp. osobním počítači, data elektronické transakce, která má být vykonána bankou. Tato data jsou přenesena prostřednictvím první komunikační infrastruktury C, s výhodou sítí Internet, do prostředí banky a nezávislého důvěryhodného systému I.

V druhém kroku 2 nezávislý důvěryhodný systém I vygeneruje k datům elektronické transakce náhodnou hodnotu JAK kódu. Hodnota JAK kódu sestává například ze čtyř číslic. Nezávislý důvěryhodný systém I vytvoří kryptografický otisk dat, která mají být podepsána a zajistí jejich šifrovaný zápis do tokenu G.

Šifrovaný zápis podepisovaných dat do tokenu G ve skutečnosti může představovat několik dílčích kroků:

a) zapnutí napájení tokenu G,
b) výběr PKI aplikace,
c) požadavek na token G na vygenerování bloku dat, která budou použita pro ustavení šifrovaného kanálu,
d) v bezpečném nezávislém důvěryhodném systému I je na základě dat získaných z předchozího bodu vygenerován šifrovací klíč (algoritmus alespoň 3DES, lépe AES, algoritmus výměny klíčů může být proprietární, popřípadě. může být použit některá ze standardizovaných metod, jako například Diffie-Hellman key agreement),
e) pomocí vygenerovaného šifrovacího klíče je sestaven blok dat pro token G, přičemž blok dat obsahuje
    i. s výhodou doplňující informace, pomocí nichž token G odvodí použitý šifrovací klíč,
    ii. s výhodou zašifrovanou informaci o maximálním počtu opakování pokusů zadání hodnoty JAK kódu uživatelem, obvykle budou povolena 3 neúspěšná zadání,
    iii. zašifrovanou hodnotu JAK kódu,
    iv. šifrovanou nebo alespoň podepsanou hodnotu hash podepisovaných dat,
    v. s výhodou elektronický podpis všech nebo vybraných částí bloku dat posílaných do tokenu G, který ověřením podpisu zjistí, zda byla data generována důvěryhodným systémem.
f) blok dat z předchozího bodu je přenesen na token G, kde je zpracován, to je, je ustaven šifrovací klíč a jsou provedeny syntaktické a kryptografické kontroly.

V kroku 3 nezávislý důvěryhodný systém I odešle hodnotu vygenerovaného JAK kódu spolu se všemi důležitými náležitostmi elektronické transakce, kterou klient zadal v kroku 1, např. typ transakce, cílový účet, částka, variabilní symbol, atd., přes druhou komunikační infrastrukturu B, například prostřednictvím GSM sítě, SMS zprávou na mobilní číslo klienta přičemž konkrétní číslo mobilního telefonu klienta je drženo v interní databázi nezávislého důvěryhodného systému I. Je velmi důležité, aby komunikace prostřednictvím GSM sítě byla dostatečně zabezpečena jak fyzicky tak aplikačně tak, aby nemohla být zneužita potencionálním útočníkem.

V následujícím kroku 6 oprávněná osoba E , resp. klient banky, současně držitel samostatného informačního zařízení F, resp. mobilního telefonu a tokenu G zkontroluje náležitosti transakce, zejména shodu s parametry transakce, které zadal v kroku 1. Současně si přečte hodnotu JAK kódu. Pokud se náležitosti platby shodují s parametry transakce, oprávněná osoba E pokračuje v kroku 7. Pokud oprávněná osoba E nehodlá například bankovní transakci potvrdit svým podpisem, přeruší celý proces.

V kroku 7 oprávněná osoba E zadáním PIN provede přihlášení na token G a zadáním JAK kódu provede potvrzení parametrů transakce tokenu G, čímž potvrdí provedení transakce. Nutno připomenout, že token G je před-inicializován z kroku 2. Token G provede kontrolu PIN, pokud není zadán správně, pak obslužný řídící kód tokenu G umožní opakované zadání PIN tak dlouho, dokud není zablokován. Podobně token G provádí kontrolu JAK kódu. Dokud není dosaženo maximálního počtu opakovaného zadání chybné hodnoty JAK kódu – obvykle 3 pokusy - je umožněno znovuzadání JAK kódu. Pokud je některý z ověřovacích kódů PIN či JAK zablokován, nebo je token G resetován či odpojen od zdroje napájení, není možné operaci dokončit. Pokud jsou všechny přístupové podmínky správně ověřeny, pokračuje se následujícím krokem 8.

Protože token G úspěšně provedl veškeré kontroly přístupových podmínek, je v rámci kroku 8 v tokenu G vypočítána hodnota elektronického podpisu dat, jejichž kryptografický otisk (hash) byl zapsán do paměti tokenu v kroku 2. Hodnota elektronického podpisu je odeslána do banky, kde je dále zpracovávána běžnými postupy.

Výhodou této varianty je to, že pro realizaci funkce vytvoření autorizovaného elektronického podpisu využívá dvě nezávislé existující komunikační infrastruktury. Uvedenou první komunikační infrastrukturu C, jíž je internetová síť pro komunikaci mezi subjektem A a nezávislým důvěryhodným systémem I na jedné straně, a oprávněnou osobou E, resp. klientem banky a jeho řídícím systémem D a tokenem G na straně druhé. První komunikační infrastruktura C zprostředkovává přenos dat k podepsání, přenos šifrovaného

JAK kódu svázaného s konkrétní transakcí a přenos vlastního podpisu dat. Dále tato varianta využívá nezávislou druhou komunikační infrastrukturu B, jíž je sít GSM, pro zasilání informačních zpráv doplněných o externě generovaný jednorázový kód JAK, který je oprávněnou osobou E přenesen do tokenu G, představovaným například čipovou kartou, kde je porovnán s kódem JAK, který před tím byl do čipové karty šifrovaně zapsán.

Další výhodou této varianty je to, že dodatečné funkce pro šifrovanou komunikaci s tokenem G a SMS notifikaci oprávněné osoba E, to je, držiteli tokenu G, zajišťuje nezávislý, důvěryhodný systém I. Subjekt A, resp. banka, tedy nemusí budovat žádné dodatečné šifrovací systémy, navíc jeden nezávislý, důvěryhodný subjekt I může poskytovat své služby více bankám , což vede ke zcela zjevným ekonomickým úsporám.

U varianty dle obrázku 3 je JAK kód generován uvnitř tokenu G, resp.čipové karty, a je použito speciální čtecí zařízení H pro zobrazení podepisovaných dat a příslušné hodnoty JAK kódu analýzou a modifikací komunikace mezi řídícím systémem D a tokenem G.

V prvém kroku 1 oprávněná osoba E, resp. klient banky zadá prostřednictvím formuláře na řídícím systémem D, to je například osobním počítači, data elektronické transakce, která má být vykonána bankou. V dalším kroku, označeném na obr.3 vztahovou značkou 4, se zadaná data přenesou prostřednictvím nezávislého informačního zařízení, kterým je speciální čtecí zařízení H, do paměti tokenu G.

Zápis dat do tokenu G může představovat několik dílčích kroků:

a) zapnutí napájení tokenu G,
b) volitelné přečtení konfiguračních dat z paměti tokenu G – konfigurační data mohou sloužit čtecímu zařízení k tomu, aby se „naučilo“ sledovat komunikaci mezi osobním počítačem a tokenem G,
c) volitelná autentizace obslužného programového vybavení osobního počítače k tokenu G – token G ví, že s ním komunikuje důvěryhodná aplikace,
d) volitelná autentizace obslužného programového vybavení čtecího zařízení k tokenu G. Autentizace může být oboustranná, to je, token G i speciální čtecí zařízení H si vzájemně důvěřují, a jejím výsledkem může být ustavení společného šifrovacího klíče sezení, tzn. token G a nezávislé informační zařízení, resp. speciální čtecí zařízení H, spolu dokáží šifrovaně komunikovat,
e) nastavení kryptografické operace a zapsání podepisovaných dat do tokenu G. V tomto okamžiku jsou podepisovaná data sledována speciálním čtecím zařízením H, tokenem G jsou hashována, správné přijetí podepisovaných dat je tokenem G indikováno a na

základě toho může speciální čtecí zařízení H, zprostředkovat jejich předání oprávněné osobě E, to je, držiteli tokenu G.

V následujícím kroku 5, po akceptaci kompletních podepisovaných dat tokenem G, je v tokenu G k těmto podepisovaným datům vygenerován náhodný JAK kód, mající např. 4 číslice s nastavením maximálního povoleného počtu neúspěšného zadání, např. na hodnotu 3. Hodnota JAK kódu je tokenem G poslána do speciálního čtecího zařízení H, přičemž komunikace může být šifrovaná, jak je uvedeno v popisu kroku 4. Čtecí zařízení H, zajistí, že se hodnota kódu JAK nedostane do řídícího systému D, kterým je osobní počítač. Hodnota JAK kódu je však sdělena oprávněné osobě E, to je držiteli tokenu G. Spolu s hodnotou JAK kódu jsou čtecím zařízením H, držiteli tokenu G sdělena, viz krok 6, i podepisovaná data, přenesená v kroku 4.

Nyní má oprávněná osoba E, to je držitel tokenu G k dispozici podepisovaná data, která byla odeslána do tokenu G k podepsání a jednorázový kód JAK, jehož zadáním může stvrdit jejich kontrolu. Pokud podepisovaná data odrážejí vůli podepisující osoby, pokračuje se krokem 7. V opačném případě může být uživatelem operace přerušena a to prostřednictvím osobního počítače nebo prostým vytažením karty ze čtecího zařízení.

Pokud jsou podepisovaná data správná, oprávněná osoba E, resp. klient banky, zadá v kroku 7 prostřednictvím osobního počítače autentizační údaje nutné pro vytvoření elektronického podpisu. Mezi autentizačními údaji je povinně hodnota JAK kódu a s výhodou hodnota PIN. Token G provede kontrolu PIN, pokud není zadán správně, pak obslužný řídící kód k tokenu G umožní opakované zadávání PIN tak dlouho, dokud není zablokován. Podobně token G provádí kontrolu JAK kódu – dokud není dosaženo maximálního počtu opakovaného zadání chybné hodnoty JAK kódu, což jsou obvykle 3 pokusy - je umožněno znovuzadání JAK kódu. Pokud je některý z ověřovacích kódů PIN i JAK zablokován nebo je token C resetován či odpojen od zdroje napájení, není možné operaci dokončit. Pokud jsou všechny přístupové podmínky správně ověřeny, pokračuje se následujícím krokem 8.

Protože token G úspěšně provedl veškeré kontroly přístupových podmínek, je v rámci kroku 8 v tokenu G je vypočítána hodnota elektronického podpisu dat, která byla zapsána do tokenu G v kroku 4. Hodnota elektronického podpisu je odeslána do banky, kde je dále zpracovávána běžnými postupy. Osobní počítač zajistí kromě odeslání hodnoty elektronického podpisu i odeslání vlastních podepisovaných dat.

Výhodou této varianty je to, že pro realizaci funkce vytvoření jednorázového autorizačního kódu JAK využívá speciální čtecí zařízení H, díky němuž je možné jednorázový autorizační kód JAK generovat přímo v tokenu G. Speciální čtecí zařízení H zajistí sdělení kódu JAK

spolu s podepisovanými daty, popřípadě jejich významnou částí, přímo oprávněné osobě E, to je, držiteli tokenu G a to prakticky bezprostředně po odeslání podepisovaných dat s požadavkem na vytvoření elektronického podpisu z osobního počítače do tokenu G, přičemž je blokována možnost přenesení autorizačního kódu JAK z tokenu G do prostředí osobního počítače. Odpadá tedy nutnost využívání externích komunikačních kanálů, jejichž provoz by mohl znamenat zvýšené náklady na provedení transakce.

Všechny výše uvedené příklady mohou být doplněny dalším pomocným prvkem pro zvýšení bezpečnosti, ale i ergonomie práce. Jedná se o doplnění mechanismů uvnitř tokenu G, které umožňují rozlišení typů vykonávání operací elektronického podpisu. Tyto operace mohou být rozděleny následujícím způsobem:

1) operace elektronického podpisu pro účely autentizace
2) operace běžného elektronického podpisu
3) operace autorizovaného elektronického podpisu s využitím JAK kódu tak, jak je to popsáno v tomto vynálezu

Pro každý typ elektronického podpisu může být použita vlastní skupina podpisových schémat. Tyto jsou definovány skupinou parametrů – např. použitý typ (resp. algoritmus) jednosměrné kompresní funkce (hash), použitý typ (resp. algoritmus) doplnění dat pro operaci elektronického podpisu (tzv. padding), použitý typ (resp. algoritmus) pro tvorbu elektronického podpisu, atd. Alternativně může být operace autorizovaného elektronického podpisu s využitím JAK kódu tak, jak je to popsáno v tomto vynálezu, indikována definovanou značkou umístěnou např. na začátku podepisovaných dat.

Vnitřní programový kód tokenu G je tak schopen přiřadit operacím vytvoření elektronického podpisu podle jednotlivých podpisových schémat i různé přístupové podmínky. Příjemce podepisovaných dat pak může výhodně ze znalosti způsobu autorizace pro vytvoření konkrétního typu podpisového schématu upravit míru důvěry v danou podepsanou zprávu.

Variantu dle obr.3 je možné výhodně realizovat i s použitím tradičních čipových karet s implementovanými mechanismy pro tvorbu elektronického podpisu, ale bez podpory funkcí vytváření autorizovaného elektronického podpisu s využitím JAK kódu tak, jak je to popsáno v tomto vynálezu. Řešení s takovouto čipovou kartou, popřípadě obdobným tradičním zařízením K pro tvorbu elektronického podpisu, je možno realizovat tak, že dodatečné funkce související s generováním a ověřováním jednorázového autorizačního kódu JAK jsou realizovány pomocným nezávislým zařízením J, které spolu s tradičním zařízením K, resp. čipovou kartou, tvoří jeden funkční celek – token G, tak jak je naznačeno na obrázku 4. Při této variantě, výhodné z hlediska zužitkování současných nástrojů tvorby elektronického

podpisu, je jednorázový autorizační kód JAK generován v rámci pomocného nezávislého zařízení J v kroku 5 tak, jak je popsáno u varianty dle obrázku 3. Krok 7, tak jak je popsán k obrázku 3 je uvnitř složeného tokenu G dále realizován v dílčích krocích následovně:

a) V dílčím kroku 7.1 jsou poslány ověřovací kódy uživatele do tradičního zařízení K pro tvorbu elektronického podpisu, kde je provedena jejich kontrola. Tento krok je možné opakovat s různými hodnotami tak dlouho, dokud nejsou tyto ověřovací kódy zablokovány. Pokud tradiční zařízení K pro tvorbu elektronického podpisu ověří platnost těchto kódů, předá v dílčím kroku 7.2 hodnotu elektronického podpisu do pomocného nezávislého zařízení J.

b) V dílčím kroku 7.3 pomocné nezávislé zařízení J pozdrží hodnotu elektronického podpisu získaného od tradičního zařízení K v dílčím kroku 7.2 do té doby, než je úspěšně ověřena hodnota jednorázového autorizačního kódu JAK, která byla generována v kroku 5. Pomocné nezávislé zařízení J umožní typicky 3 pokusy o ověření hodnoty jednorázového autorizačního kódu JAK. Pokud je vyčerpán maximální počet pokusů o ověření jednorázového autorizačního kódu JAK je navrácení hodnoty elektronického podpisu zablokováno.

c) Pokud byl zadán jednorázový autorizační kód JAK správně a je v dílčím kroku 7.3 ověřen, pomocné nezávislé zařízení J umožní předání hodnoty elektronického podpisu do externího prostředí, což je v obrázku naznačeno jako dílčí krok 7.4, který de facto odpovídá kroku 8 varianty dle obrázku 3.

Průmyslová využitelnost

Metoda pro autorizované vytváření elektronického podpisu dat podle vynálezu je průmyslově opakovatelně využitelné řešení a najde využití především v aplikacích, kde je nutné zajistit silný princip neodmítnutelnosti odpovědnosti. Takovými aplikacemi jsou zejména aplikace elektronického bankovnictví, které přímo realizují finanční transakce a jsou tedy velmi zajímavé pro potencionální útočníky. Oprávněná osoba E, resp.klient banky, má díky vynálezu možnost ověřit, jaké operace skutečně provádí a subjekt A, resp. banka, má vyšší důvěru v takto podepsanou transakci.

Analogicky lze systém využít i např. v elektronické komunikaci občana se státní správou, či jiných systémech, které jsou založeny na elektronickém podpisu.

PATENTOVÉ NÁROKY

1. Způsob vytváření autorizovaného elektronického podpisu oprávněné osoby (E), kdy podepisovaná data, která mají být opatřena elektronickým podpisem se zadají do řídícího systému (D), **vyznačující se tím**, že podepisovaná data se uloží do vnitřní paměti tokenu (G), jehož držitelem je oprávněná osoba (E), přičemž se podepisovaná data do tokenu (G) uloží v kompletní podobě a/nebo v podobě kryptografického otisku, načež před realizací elektronického podpisu se vygeneruje dodatečný jednorázový autorizační kód JAK, patřící k podepisovaným datům, podepisovaná data se společně s jednorázovým autorizačním kódem JAK sdělí prostřednictvím samostatného, nezávislého informačního zařízení, jež není součástí řídícího systému (D), oprávněné osobě (E), která provede jejich kontrolu, poté se jednorázový autorizační kód JAK, s výhodou spolu s dalšími ochrannými prvky, zadají do tokenu (G), kde se použijí jako přístupová podmínka pro vytvoření a vrácení hodnoty elektronického podpisu, přičemž v tokenu (G) se provede kontrola, zda jednorázový autorizační kód JAK, a další ochranné prvky, byly zadány správně, přičemž v kladném případě token (G) vytvoří hodnotu elektronického podpisu, která se odešle s daty do subjektu (A), pro nějž je autorizovaný elektronický podpis vytvářen, zejména do banky nebo jiného subjektu.

2. Způsob podle nároku 1, **vyznačující se tím**, že jednorázový autorizační kód JAK se vygeneruje v tokenu (G) a sdělí se oprávněné osobě (E) spolu s podepisovanými daty prostřednictvím samostatného, nezávislého informačního zařízení, kterým je čtecí zařízení (H), přičemž se blokuje přenos jednorázového autorizačního kódu JAK do řídícího systému (D).

3. Způsob podle nároku 1, **vyznačující se tím**, že jednorázový autorizační kód JAK se vygeneruje subjektem (A), pro nějž je autorizovaný elektronický podpis vytvářen, nebo jiným,na subjektu (A) nezávislým a věrohodným systémem (I), v zašifrované podobě se přenese spolu s podepisovanými daty do tokenu (G), přičemž podepisovaná data jsou kryptograficky chráněna a token (G) provede kontrolu, zda pocházejí ze stejného systému jako vygenerovaný jednorázový autorizační kód JAK a taktéž se podepisovaná data i jednorázový autorizační kód (JAK) subjektem (A) či věrohodným systémem (I) sdělí oprávněné osobě (E) prostřednictvím samostatného, nezávislého informačního zařízení, které je neovlivnitelné řídícím systémem (D), s výhodou tak, že se zobrazí na displeji zařízení, kterým je výhodně mobilní telefon (F) oprávněné osoby (E).

4. Způsob podle některého z nároků 1 až 3, **vyznačující se tím**, platnost jednorázového autorizačního kódu JAK je omezena jen na sezení, v jehož rámci je možné data podepsat, přičemž platnost jednorázového autorizačního kódu JAK je ukončena odpojením napájení tokenu (G), resetováním tokenu (G) či inicializací nového sezení pro vytvoření elektronického podpisu.

5. Způsob podle některého z nároků 1 až 4, **vyznačující se tím**, že vytvoření autorizovaného elektronického podpisu konkrétních dat se zablokuje, nebo se zabrání navrácení hodnoty elektronického podpisu, pokud se po provedení kontroly v tokenu (G) zjistí překročení povoleného počtu nesprávného zadání jednorázového autorizačního kódu JAK či dalších ochranných prvků.

6. Zařízení k provádění způsobu podle některého z nároků 1, 2, 4 a 5, **vyznačující se tím**, že řídící systém (D) je přes první komunikační infrastrukturu (C) propojen se subjektem (A), pro nějž je elektronický podpis vytvářen, dále je řídící systém (D) obousměrně propojen s nezávislým informačním zařízením, jímž je s výhodou čtecí zařízení (H), jež je obousměrně propojeno s tokenem (G) a je upraveno pro přenos dat mezi řídícím systémem (D) a tokenem (G) a pro předání vybraných přenášených podepisovaných dat oprávněné osobě (E), která je držitelem tokenu (G) a dále je upraveno pro zabránění přenosu vybraných citlivých dat z tokenu (G) do řídícího systému (D).

7. Zařízení k provádění způsobu podle některého z nároků 1, 3, 4 a 5, **vyznačující se tím**, že řídící systém (D) je přes první komunikační infrastrukturu (C) propojen se subjektem (A), pro nějž je vytvářen elektronický podpis, přičemž subjekt (A) je jednak propojen přes druhou komunikační infrastrukturu (B), nezávislou na první komunikační infrastruktuře (C), se samostatným informačním zařízením (F) pro předání jednorázového autorizačního kódu JAK a podepisovaných dat oprávněné osobě (E), která je držitelem tokenu (G) a jednak přes první komunikační infrastrukturu (C) a řídící systém (D) s tokenem (G).

8. Zařízení k provádění způsobu podle některého z nároků 1, 3, 4 a 5, **vyznačující se tím**, že řídící systém (D) je prostřednictvím první komunikační infrastruktury (C) propojen se subjektem (A) a s na subjektu (A) nezávislým a věrohodným systémem (I), pro generování a/nebo pro zašifrování jednorázového autorizačního kódu JAK a doplnění ochranných prvků k podepisovaným datům, přičemž systém (I) je jednak propojen přes druhou komunikační infrastrukturu (B), nezávislou na první komunikační infrastruktuře (C),

se samostatným informačním zařízením (F) pro předání jednorázového autorizačního kódu JAK a podepisovaných dat oprávněné osobě (E), která je držitelem tokenu (G) a jednak přes první komunikační infrastruktury (C) a řídící systém (D) s tokenem (G).

9. Zařízení podle nároku 8, **vyznačující se tím**, že nezávislý a věrohodný systém (I) pro zašifrování je součástí subjektu (A) nebo jiného nezávislého subjektu.

10. Zařízení podle některého z nároků 6, 7, 8 nebo 9, **vyznačující se tím**, že první komunikační infrastrukturou (C) je internetová síť.

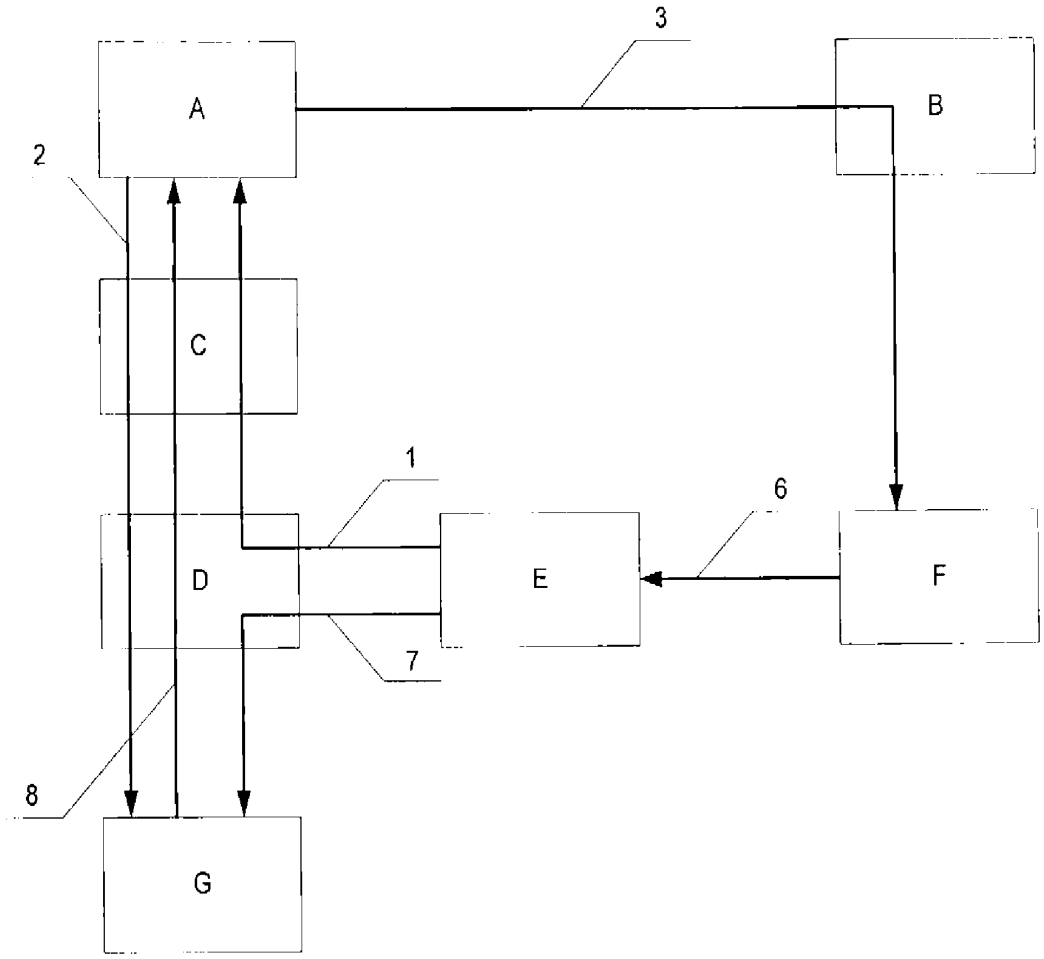
11. Zařízení podle nároku z nároků 7, 8, 9 nebo 10 **vyznačující se tím**, že druhou komunikační infrastrukturou (B) je GSM síť.

12. Zařízení podle některého z nároků 1 až 11, **vyznačující se tím**, že řídícím systémem (D) je osobní počítač.

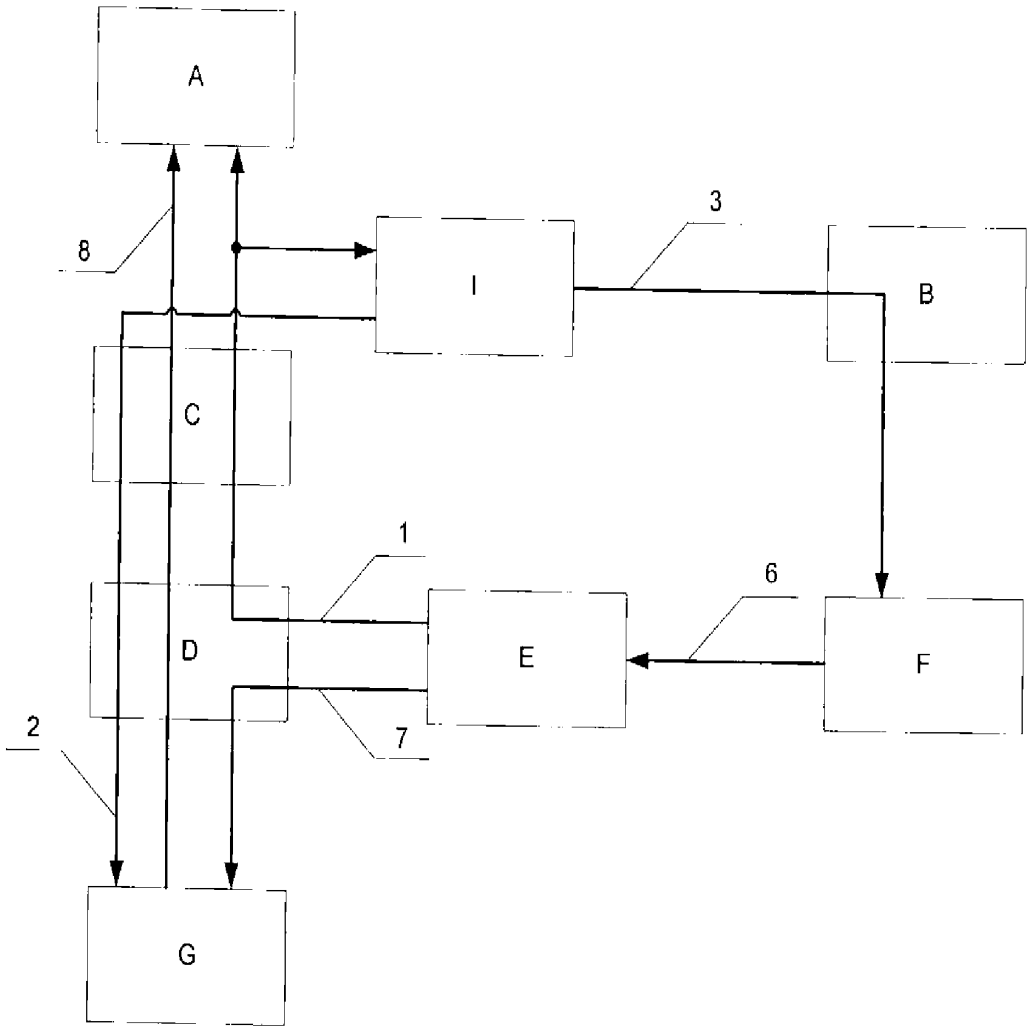
13. Zařízení podle některého z nároků 1 až 12, **vyznačující se tím**, že tokenem (G) je čipová karta.

14. Zařízení podle některého z nároků 1 až 12, **vyznačující se** tím, že token (G) je tvořen nezávislým pomocným zařízením (J) a tradičním zařízením (K) pro tvorbu elektronického podpisu , které nemá podporu metod generování a ověření JAK kódu, přičemž nezávislé pomocné zařízení (J) je upraveno pro implementaci doplňujících funkcí, zejména realizaci metody pro generování a ověření JAK kódu.

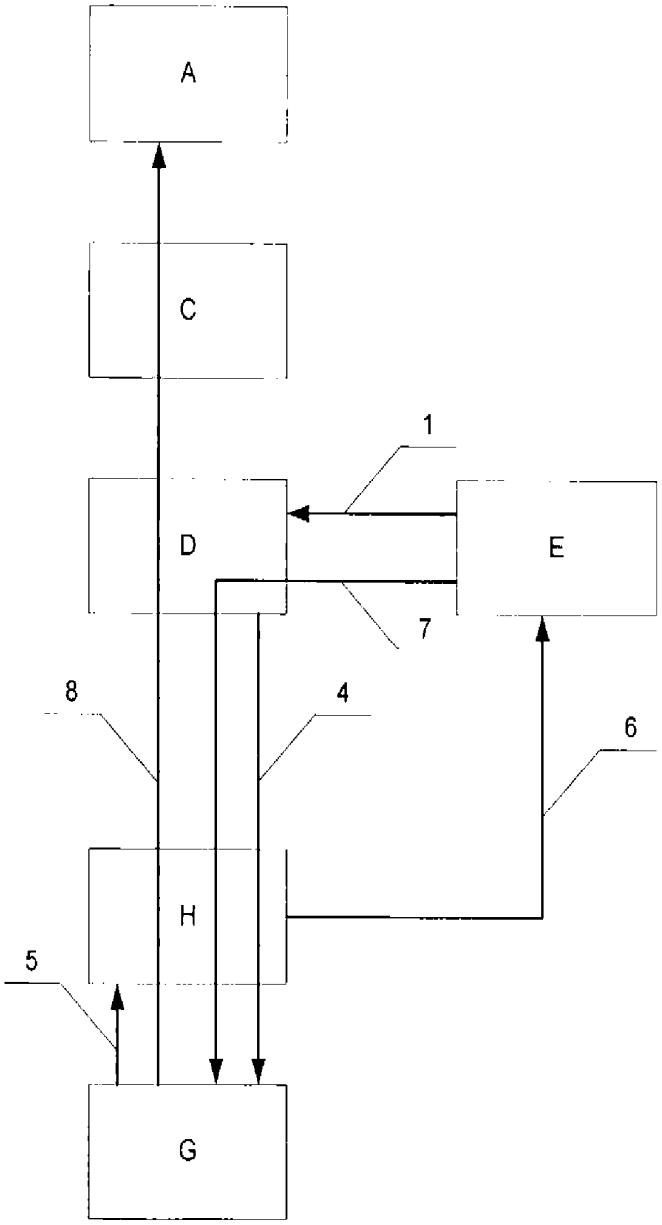
Obr. 1



Obr. 2



Obr. 3



Obr. 4