

# PATENTOVÝ SPIS

(19)  
ČESKÁ  
REPUBLIKA



ÚŘAD  
PRŮMYSLOVÉHO  
VLASTNICTVÍ

(21) Číslo přihlášky: **2002-3361**  
(22) Přihlášeno: **09.03.2001**  
(30) Právo přednosti: **10.03.2000 SE 0000795**  
(40) Zveřejněno: **14.05.2003**  
(Věstník č. 5/2003)  
(47) Uděleno: **08.03.2010**  
(24) Oznámení o udělení ve Věstníku: **14.04.2010**  
(Věstník č. 15/2010)  
(86) PCT číslo: **PCT/SE2001/000501**  
(87) PCT číslo zveřejnění: **WO 2001/066888**

(11) Číslo dokumentu:

**301 556**

(13) Druh dokumentu: **B6**

(51) Int. Cl.:  
**G07C 9/00 (2006.01)**

(56) Relevantní dokumenty:

US 6005487 A; US 4736419 A; WO 98/25000 A1; US 4912310 A; WO 90/15211 A1; EP 0410024 A1.

(73) Majitel patentu:

ASSA ABLOY AB, Stockholm, SE

(72) Původce:

Lidén Inge, Eskilstuna, SE  
Norberg Rolf, Täby, SE  
Magnusson Björn, Tumba, SE  
Sivonen Hannu, Marjovaara, FI  
Brennecke Gudrun, Berlin, DE  
Chanel Christophe, Berlin, DE  
Krühn Jürgen, Berlin, DE  
Kikebusch Bernd, Berlin, DE  
Lefebvre Arnaud, Troyes, FR

(74) Zástupce:

JUDr. Zdeňka Korejzová, Spálená 29, Praha 1, 11000

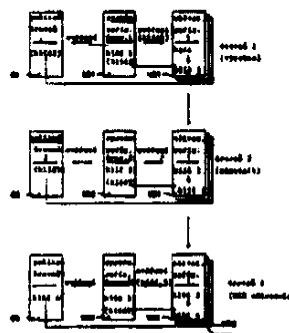
(54) Název vynálezu:

**Způsob autorizace uživatelského zařízení  
systému klíče a zámku a systém klíče a zámku**

(57) Anotace:

Způsob autorizace uživatelského zařízení systému klíče a zámku zahrnuje kroky provedení ověřovacího procesu, mezi uživatelským zařízením a prvním systémovým zařízením s použitím prvního kódovacího klíče, a v případě, že ověřovací proces byl úspěšný, provedení softwarové operace prvním systémovým zařízením, ve které se první kódovací klíč, uložený v uživatelském zařízení, nahradí druhým kódovacím klíčem.

Dále je popsán systém klíče a zámku, který zahrnuje alespoň jedno systémové zařízení (SD1 až SD3) mající elektronické obvody zahrnující elektronickou paměť upravenou pro uložení trvalého elektronického kódovacího klíče, a počítačový programový software upravený pro změnu proměnného elektronického kódovacího klíče uživatelského zařízení z prvního kódovacího klíče na druhý kódovací klíč v důsledku úspěšného ověřovacího procesu provedeného mezi zámkem nebo uživatelským klíčem, majícím uložený proměnný elektronický kódovací klíč, a systémovým zařízením majícím shodný kódovací klíč jako uvedený zámek nebo uživatelský klíč.



**CZ 301556 B6**

**Způsob autorizace uživatelského zařízení systému klíče a zámku a systém klíče a zámku**Oblast techniky

5

Předkládaný vynález se týká způsobu autorizace uživatelského zařízení systému klíče a zámku, přičemž uživatelským zařízením je uživatelský klíč nebo zámek systému hlavního klíče, a přičemž tento způsob zahrnuje následující kroky: vytvoření uživatelského zařízení majícího elektronické obvody, vytvoření prvního systémového zařízení majícího elektronické obvody a používaného v první úrovni systému klíče a zámku, a uložení prvního kódovacího klíče v prvním uživatelském zařízení a v prvním systémovém zařízení. Tento vynález se dále týká systému klíče a zámku, který zahrnuje: množství uživatelských zařízení zahrnujících: množství uživatelských klíčů majících elektronické obvody zahrnující elektronickou paměť upravenou pro uložení proměnného elektronického kódovacího klíče, a množství zámků majících elektronické obvody zahrnující elektronickou paměť upravenou pro uložení proměnného elektronického kódovacího klíče, přičemž uživatelský klíč a zámek jsou spolu provozuschopné pouze tehdy, když jsou v tomto uživatelském klíči a zámku uloženy shodné kódovací klíče.

20 Dosavadní stav techniky

V současnosti jsou již známy elektromechanické zamykací systémy, u kterých jsou klíče přiděleny různým uživatelům běžným způsobem podobným způsobu, jakým jsou klíče distribuovány v mechanickém zamykacím systému. Toto distribuování se ale obtížně provádí a je velmi těžkopádnou procedurou distribuovat nové klíče. Rovněž zde vždy existuje nebezpečí, že neautorizovaná osoba získá systémový klíč, což potom vede k bezpečnostním rizikům, a podobně.

Dalším problémem je, že elektronické kódy mohou být kopírovány, například „záznamem“ kódu prostřednictvím čtecího zařízení, přičemž kopie mohou být přítomny v systému klíčů, aniž by o tom měl povědomí vlastník systému.

Ještě dalším problémem dosavadního stavu techniky je, že polotovary klíčů mohou být použity kýmkoliv, což s sebou nese bezpečnostní rizika.

35 US patentový dokument US 6,005,487 (Hyatt, Jr. a kol.), popisuje elektronický bezpečnostní systém zahrnující elektronický zamykací mechanismus a elektronický klíč. Aby se vyloučil požadavek na nákladné obnovení (výměnu) klíčů v případě ztráty klíče, nebo aby se vyloučila možnost vnitřního podvodu a krádeže, umožňuje systém podle tohoto patentového dokumentu US 6,005,487 změnu identifikačního kódu klíče nebo zámku. Výše zmiňované problémy dosavadního stavu techniky, ale nejsou tímto systémem řešeny.

45 Cílem předkládaného vynálezu je vytvořit zařízení elektromechanického klíče a zámku v úvodu zmiňovaného typu a použít v systému, ve kterém distribuování a autorizace klíčů a zámků mezi výrobcem, distributorem a zákazníkem mají vysokou úroveň bezpečnosti.

Dalším cílem předkládaného vynálezu je vytvořit zařízení elektromechanického zámku, u kterého je usnadněna distribuce a autorizace klíčů.

50 Dalším cílem vynálezu je vytvořit zařízení klíče, které lze obtížně kopírovat bez povědomí vlastníka systému.

Dalším cílem vynálezu je vytvořit polotovar klíče, který je omezen dokud se týká jeho použití na omezený počet distributorů.

Dalším cílem vynálezu je zajistit snadné a bezpečné přidávání klíčů a zámků do zamykacího systému.

5 Dalším cílem vynálezu je navrhnout způsob a systém pro ukládání a zobrazování informací o systému hlavního klíče bezpečným způsobem.

Dalším cílem vynálezu je navrhnout způsob a systém pro výměnu informací mezi výrobcem, distributorem a koncovým uživatelem zařízení klíče a zámku.

10

#### Podstata vynálezu

Vynález je založen na zjištění, že výše zmiňované problémy dosavadního stavu techniky mohou být vyřešeny prostřednictvím vytvoření a výměny elektronických kódů v klíčích a zámcích, při-  
15 čemž tyto kódy jsou použity pro kódovanou komunikaci mezi klíči a zámky a mezi různými stranami účastnými při vytváření a údržbě zamykacího systému.

Podle vynálezu je tedy navržen způsob v úvodu uvedeného typu, jehož podstata spočívá v tom, že zahrnuje kroky provedení ověřovacího procesu mezi uživatelským zařízením a prvním systé-  
20 movým zařízením s použitím prvního kódovacího klíče, a v případě, že ověřovací proces byl úspěšný, provedení softwarové operace prvním systémovým zařízením, ve které se první kódovací klíč, uložený v uživatelském zařízení, nahradí druhým kódovacím klíčem, přičemž druhý kódovací klíč se uloží v druhých systémových zařízeních a dalších uživatelských zařízeních pou-  
žitých v druhé úrovni systému klíče a zámku, čímž se dosáhne toho, že uživatelské zařízení je  
25 provozuschopné s druhými systémovými a dalšími uživatelskými zařízeními.

Výhodně se během kroku náhrady prvního kódovacího klíče, uloženého v uživatelském zařízení, druhý kódovací klíč dodá prostřednictvím prvního systémového zařízení.

30 Výhodně se během kroku náhrady prvního kódovacího klíče, uloženého v uživatelském zařízení, druhý kódovací klíč dodá prostřednictvím počítače.

Způsob podle vynálezu výhodně dále zahrnuje přidavný krok dodání druhého kódovacího klíče do počítače přes síť, jako jsou lokální síť a veřejné telefonní síť.

35

Výhodně je prvním systémovým zařízením systémový klíč systému hlavního klíče.

Výhodně je uživatelským zařízením uživatelský klíč systému hlavního klíče.

40 Výhodně je uživatelským zařízením je zámek systému hlavního klíče.

Výhodně jsou elektronické kódovací klíče nečitelné z vnějšku uvedených elektronických obvodů.

Podle vynálezu je dále navržen systém klíče a zámku, v úvodu uvedeného typu, jehož podstata  
45 spočívá v tom, že zahrnuje alespoň jedno systémové zařízení mající elektronické obvody zahrnující elektronickou paměť upravenou pro uložení trvalého elektronického kódovacího klíče, a počítačový programový software upravený pro změnu proměnného elektronického kódovacího klíče uživatelského zařízení z prvního kódovacího klíče na druhý kódovací klíč v důsledku úspěšného ověřovacího procesu provedeného mezi zámkem nebo uživatelským klíčem, majícím  
50 uložený proměnný elektronický kódovací klíč, a systémovým zařízením majícím shodný kódovací klíč jako uvedený zámek nebo uživatelský klíč, přičemž druhý kódovací klíč je uložen v druhých systémových zařízeních a uživatelských zařízeních, používaných v druhé úrovni systému klíče a zámku, čímž jsou uživatelská zařízení provozuschopná s těmito druhými systémovými a  
uživatelskými zařízeními.

55

V následujícím popisu bude předkládán vynález poněkud podrobněji popsán prostřednictvím příkladných provedení ve spojení s odkazy na připojené výkresy.

## 5 Přehled obrázků na výkresech

- Obr. 1 znázorňuje schéma vysvětlující základní myšlenku předkládaného vynálezu;
- Obr. 2 znázorňuje celkový pohled na hierarchický zamykací systém se zařízeními klíče a zámku podle vynálezu;
- 10 Obr. 3a znázorňuje informační prvky zařízení klíče podle vynálezu;
- Obr. 3b znázorňuje informační prvky zařízení zámku podle vynálezu;
- Obr. 4 znázorňuje příklad informačního toku v systému, který je znázorněn na obr. 2;
- Obr. 5 znázorňuje přehled kódovacích prvků elektronického klíče v zařízení klíče a zámku podle vynálezu;
- 15 Obr. 6 znázorňuje schéma ilustrující zabezpečení datové výměny mezi výrobcem, distributorem a zákazníkem;
- Obr. 7 znázorňuje přehled kódování databáze, použitého podle vynálezu; a
- Obr. 8 znázorňuje příklad kódovacích tabulek databázového souboru.

20

## Příklady provedení vynálezu

Nyní budou popsána výhodná provedení předkládaného vynálezu. Aby bylo dosaženo zcela jasného popisu, bude výraz „klíč“ ožrejměn přidáním výrazu „fyzický“, pokud slovo klíč má označovat fyzická klíč, to jest mechanický klíč upravený pro použití se zámkem, a nebo přidáním  
25 výrazu „elektronický“ nebo „kódovací“, pokud slovo klíč má označovat elektronický klíč, jako je kódovací klíč.

Navíc je použita předpona „e“ pro označení kódované informace a předpona „d“ pro označení dekódované informace. Použitý kódovací klíč následuje za touto předponou. Tak například výraz  
30 eKx(Soubor1) označuje Soubor1 kódovaný kódovacím klíčem „Kx“.

V tomto popisu je někdy použit výraz „zařízení“. Zařízení v kontextu předkládaného vynálezu je třeba interpretovat jako zařízení klíče nebo zámku.

35

Nejprve bude vysvětlena základní myšlenka předkládaného vynálezu ve spojení s odkazy na obr. 1, který ilustruje schéma různých částí zamykacího systému podle vynálezu. Jsou znázorněny tři „úrovně“ zamykacího systému, označené „výrobce“, „zámečník“ respektive „uživatel MKS“. V každé úrovni je systémové zařízení a případně počítač v jedné nebo více úrovních.  
40 V různých úrovních jsou znázorněna uživatelská zařízení, jako jsou klíče a/nebo zámky. „Uživatelské zařízení 1“ je ale stejné zařízení ve všech úrovních, ačkoliv v různých „režimech“.

Každé systémové a uživatelské zařízení má v sobě uložený skrytý kódovací klíč, „klíč1“, „klíč2“, a tak dále. Tyto kódovací klíče jsou použity pro ověřovací procesy mezi systémovými a  
45 uživatelskými zařízeními a rovněž mezi různými uživatelskými zařízeními, to jest mezi klíči a zámky na úrovni koncového uživatele. Kódovací klíče, uložené v uživatelských zařízeních, jsou proměnné, to znamená, že mohou být měněny prostřednictvím systémového zařízení, případně ve spojení s počítačovým softwarem, jak bude vysvětleno v následujícím popisu.

Nejprve tedy například uživatelské zařízení UD1, uložené na úrovni 1, má vytvořen kódovací klíč „klíč1“ během výroby polotovaru klíče. Když má být uživatelské zařízení 1 předáno do úrovně 2, je inicializován ověřovací proces mezi systémovým zařízením SD1 a uživatelským zařízením UD1 s použitím kódovacího klíče „klíč1“. Pokud je tento ověřovací proces úspěšný, „klíč1“,  
50

uložený v uživatelském zařízení, je nahrazen kódovacím klíčem „klíč2“ a proces je ukončen. Nový kódovací klíč „klíč2“ může být dodán buď samotným systémovým zařízením nebo případně počítačem C1. Žádný další úspěšný ověřovací proces nemůže být následně proveden na této úrovni mezi příslušným uživatelským zařízením a systémovým zařízením, protože kódovací klíče si neodpovídají.

Uživatelské zařízení může být nyní bezpečně dodáno do úrovně 2, úrovně „zámečník“, protože případný podvádějící účastník, který zachytí uživatelské zařízení, nebude schopen použít toto uživatelské zařízení bez znalosti skrytého kódovacího klíče uloženého v tomto zařízení, to jest kódovacího klíče „klíč2“.

Na úrovni 2 se provede odpovídající procedura jako v úrovni 1 předtím, než se uživatelské zařízení dodá koncovému uživateli, to znamená, že kódovací klíč „klíč2“, uložený v uživatelském zařízení, se nahradí kódovacím klíčem „klíč3“ prostřednictvím systémového zařízení SD2, případně ve spolupráci s počítačem C2.

Uživatelské zařízení, které se dostává do úrovně koncového uživatele, to jest úrovně 3, nemůže být použito, dokud nebylo autorizováno prostřednictvím systémového zařízení SD3 stejným způsobem jako v úrovni 2. To znamená, že kódovací klíč „klíč3“ se nahradí kódovacím klíčem „klíč4“ po úspěšném ověřovacím procesu s použitím kódovacího klíče „klíč3“. Všechna uživatelská zařízení, to jest všechny klíče a zámky systému hlavního klíče, musí projít tímto procesem předtím, než mohou být použita. To také znamená, že všechna „aktivovaná“ uživatelská zařízení mají v sobě uložen kódovací klíč „klíč4“ a mohou tudíž provádět úspěšné ověřovací procesy vzájemně mezi sebou. To zajišťuje úplnou bezpečnost při distribuování klíčů nebo zámků pro systém hlavního klíče koncového uživatele.

Zamykací systém, zahrnující zařízení klíče a zámku podle předkládaného vynálezu, bude nyní detailně popsán ve spojení s odkazy na obr. 2, který znázorňuje typické rozložení hardwarových a softwarových nástrojů mezi různými úrovněmi hierarchie, přesněji mezi zákazníkem 100, distributorem 200 a výrobcem 300.

#### Uživatelské klíče

V systému zákazníka 100 existuje několik uživatelských klíčů 101 upravených pro použití s množstvím zámků 20. Uživatelské klíče a zámky dohromady tvoří systém hlavního klíče (MKS). Každý klíč má unikátní individuální elektronický kód řídící jeho funkci. Elektronický kód je rozdělen na různé segmenty pro použití výrobcí, distributory a zákazníky. Je vytvořen veřejný (otevřený) segment pro otevřené (veřejné) informace a je rovněž vytvořen tajný segment pro tajné informace. Segmenty jsou dále rozděleny do různých prvků nebo položek elektronického kódu. Elektronický kód klíče je dále diskutován níže ve spojení s popisem chráněných režimů.

#### Programovací a autorizační klíč

Pro systém zákazníka 100 existuje alespoň jeden zákaznický, programovací a autorizační klíč (C–klíč) 102. C–klíče společně s D–klíči a M–klíči (viz popis níže) budou v tomto dokumentu rovněž označovány jako systémové klíče (SYS–klíče).

#### Zákaznická programovací skříň

Na straně zákazníka je programovací skříň 106, upravená pro spojení s počítačem (PC) 104 přes, například, sériové rozhraní. Tato programovací skříň zahrnuje statickou čtečku 107 a je použita pro programování v systému zákazníka. Statická čtečka 107 je čtečkou klíčů bez blokovacího mechanismu a tudíž zahrnuje elektronické obvody, a tak dále, pro čtení a programování klíče.

Ačkoliv na obrázku je znázorněna zákaznická programovací skříň 106, tato programovací skříň 106 může být vypuštěna ve velmi malých zamykacích systémech.

#### Zákaznický software

5

Zákazník má přístup k osobnímu počítači 104 pracujícímu se zákaznickým administračním softwarem (C-software) pouze s otevřenými (veřejnými) systémovými informacemi. C-software tudíž v tak zvané zamykací mapě udržuje přehled o tom, které klíče jsou autorizovány ve kterých zámecích příslušného systému hlavního klíče. Tajné identity (viz níže) všech klíčů jsou ale uloženy v kódované podobě, která může být čtena pouze prostřednictvím systémového klíče.

10

#### Autorizační klíč pro distributora

15

Pro distributora zamykacího systému, kterým může být například zámečník, je vytvořen autorizační klíč (D-klíč) 202 distributora.

#### Programovací skříň distributora

20

Na straně distributora je rovněž programovací skříň 206 upravená pro spojení s počítačem (PC) 204 přes například sériové rozhraní. Tato programovací skříň 206 může být shodná nebo podobná jako skříň popsaná ve spojení se systémem zákazníka 100.

#### Software distributora

25

Distributor má speciální počítačový software (D-software) pro osobní počítač 204. D-software obsahuje otevřenou (veřejnou) část pro zobrazování otevřených systémových informací a pro konstruování změn, a tak dále. Tento D-software rovněž obsahuje tajnou část obsahující autorizační kódy a tajná klíčová slova použitá v systému. D-software rovněž podporuje kódovanou komunikaci s počítačem 304 výrobce zamykacího systému, prostřednictvím například modemového spojení 208, jak bude podrobněji diskutováno v popisu níže.

30

Software distributora používá jako modul registr klíčů/zámek, který popisuje systém zákazníka. Tímto způsobem může distributor pracovat transparentně, jako kdyby software distributora a zákazníka byly jedním systémem. To je pro distributora nezbytné, pokud má být úzce spojen s obsluhou zákaznického systému.

35

#### Autorizační klíč pro výrobce

40

Pro výrobce zamykacího systému je vytvořen autorizační klíč (M-klíč) 302 výrobce.

#### Programovací skříň výrobce

45

Na straně výrobce je rovněž programovací skříň 306 podobná programovací skříni 206 distributora a upravená pro spojení s počítačem (PC) 304.

#### Software výrobce

50

Výrobce má přístup k osobnímu počítači 304, který pracuje se softwarem (M-software) s úplnou autorizací pro operace týkající se přidávání a rušení klíčů a zámek.

#### Informační prvky

55

Všechny klíče a zámky mají unikátní elektronickou identitu nebo kód zahrnující několik informačních prvků řídících funkci klíčů a zámek. Tyto informační prvky klíčů nebo zámek budou nyní popsány ve spojení s odkazy na obr. 3a respektive obr. 3b.

Elektronický kód je rozdělen na různé segmenty pro použití výrobcí, distributory a zákazníky. Některé veřejné prvky jsou společné pro zařízení MKS, přičemž je také vytvořen tajný segment pro tajné informace, který je vždy individuální pro skupinu.

5

Každý elektronický kód klíče zahrnuje následující části:

- veřejnou identifikaci klíče (PKID) zahrnující
  - identifikaci výrobce (M)
  - identifikaci systému hlavního klíče (MKS)
  - 10 • identifikaci funkce (F)
  - identifikaci skupiny (GR)
  - unikátní identitu (UID)
- kódovací klíč ( $K_{DES}$ )
- tajnou identifikaci klíče (SKID) zahrnující
  - 15 • tajnou identifikaci skupiny (SGR)

Rovněž každý elektronický kód zámku zahrnuje následující části:

- veřejnou identifikaci zámku (PLID) zahrnující
  - identifikaci výrobce (M)
  - 20 • identifikaci systému hlavního klíče (MKS)
  - identifikaci funkce (F)
  - identifikaci skupiny (GR)
  - unikátní identitu (UID)
- kódovací klíč ( $K_{DES}$ )
- 25 • tajnou identifikaci klíče (SLID) zahrnující
  - tajnou identifikaci skupiny (SGR)

Základní prvky kódů budou nyní popsány poněkud podrobněji.

30 M – výrobce

M identifikuje výrobce systému hlavního klíče. Každému výrobcí 300 využívajícímu předkládaný vynález je tudíž přidělen unikátní M-kód identifikující klíče a zámky pocházející od tohoto výrobce.

35

MKS – systém hlavního klíče

MKS identifikuje různé systémy hlavního klíče zákazníků 100. Zámek bude akceptovat uživatelský klíč nebo C-klíč, pouze když tyto prvky budou mít stejný MKS-kód.

40

F – funkce

F identifikuje úlohu zařízení, to jest zda je zámkem, uživatelským klíčem, C-klíčem, D-klíčem, M-klíčem, a tak dále.

45

GR – skupina

GR je celé číslo identifikující skupinu zařízení. GR je unikátní v každém MKS a začíná číslem 1 a dále vždy s přírůstkem 1.

50

## UID – unikátní identita

UID identifikuje různé uživatele ve skupině. UID je unikátní v každé skupině, začíná číslem 1 a dále vždy s přírůstkem 1. Kombinace identifikátoru skupiny a unikátní identity tedy unikátně identifikuje zařízení v MKS.

## $K_{DES}$ – kódovací klíč

$K_{DES}$  zahrnuje náhodně generovaný kódovací klíč. Ve výhodném provedení je použit kódovací algoritmus DES, částečně z důvodu jeho rychlosti, a výhodně algoritmus trojnásobný DES (3DES). Existuje několik režimů činnosti DES kódování, přičemž dva režimy jsou výhodné pro předkládaný vynález: ECB (zápis elektronického kódu) a CBC (řetězení šifrových bloků).

$K_{DES}$  je shodný ve všech zařízeních systému hlavního klíče.

$K_{DES}$  není žádným způsobem čitelný z vnějšku a je použit pouze algoritmy vykonávanými uvnitř zařízení klíče a zámku. To je velmi důležitý znak, protože to vylučuje možnost kopírování klíče přečtením obsahu jeho paměti. Navíc je  $K_{DES}$  přítomen pouze v klíčích ve funkčním režimu, viz diskuse v popisu níže a chráněném režimu.

$K_{DES}$  je použit v autorizačních procesech probíhajících mezi různými zařízeními. Aby tedy klíč byl schopen pracovat se zámkem, jak klíč tak zámek musí mít stejný  $K_{DES}$ . V opačném případě autorizační proces není úspěšný.

## SGR – tajná skupina

SGR je náhodně generované číslo, které je stejné pro jednu skupinu. Shora zmiňované informační prvky a rovněž další elektronické datové informace, použité v systému klíče a zámku podle předkládaného vynálezu, jsou samozřejmě informacemi zásadními pro funkci systému. Proto, aby se zajistila integrita dat, je pro některá z dat použit MAC (ověřovací kód zpráv). V zařízení klíče nebo zámku, je MAC použit pro každý autorizační výpis v čipu používajících  $K_{DES}$ . MAC je rovněž použit pro některé datové prvky předtím, než je zařízení uvedeno do funkčního režimu (viz níže) a rovněž pro některé další datové prvky. V C-software, D-software nebo M-software je MAC použit pro některé nekódované datové soubory.

Systém klíče a zámku podle předkládaného vynálezu vykazuje velmi vysokou úroveň bezpečnosti. Bezpečnostní architektura je založena na skutečnosti, že systémový klíč, to jest C-klíč, D-klíč nebo M-klíč, může pracovat s mnoha různými software. Není tudíž snadné změnit ověřovací kódovací klíč pro každé provedené ověření. Typický informační tok v hierarchickém systému, znázorněném na obr. 2, je ilustrován na obr. 4. Tento obrázek příkladně ilustruje složitost systému a informací vyměňovaných mezi různými úrovněmi, to jest výrobcem, distributorem a zákazníkem.

Ve znázorněném příkladu si zákazník 100 přeje přidání uživatelského klíče do svého systému hlavního klíče (krok 401). S použitím plánovacího software (v kroku 402) je informace týkající se požadovaných změn přenesena o výrobcí prostřednictvím, například, modemového spojení 108 a 308, viz obr. 2. Na straně výrobce 300 je s použitím M-software v počítači 304 (krok 403) přistoupeno k databázi M-software (krok 404) prostřednictvím použití M-klíče (krok 405). Databáze M-software je potom aktualizována a příslušné informace jsou vyslány do D-software (krok 406), například prostřednictvím modemového spojení 308 a 208.

Na straně distributora 200, je přistoupeno k databázi D-software v počítači 204 (krok 407) a tato databáze je aktualizována s použitím D-klíče 202 (krok 408). Vytvoří se zařízení v chráněném režimu, příslušející příslušnému MKS, a toto zařízení se naprogramuje prostřednictvím D-klíče 202 a programovací skříň 206.

Na straně zákazníka 100 C-software v počítači 104 přijímá informace od distributora (krok 409), například prostřednictvím modemového spojení. Je přístupováno k databázi C-software (krok 410), tato databáze je aktualizována a je dodáno nové zařízení distributorem (krok 411), které je naprogramováno prostřednictvím programovací skříně 106 a C-klíče 102 (krok 412). Když toto chráněné zařízení bylo uvedeno do funkčního režimu (krok 413), je na tuto skutečnost upozorněn M-software v počítači 304 a je příslušně aktualizována databáze M-software.

Čtenář snadno nahlédne složitost všech těchto operací a potřebu jednoduchého a ještě bezpečného způsobu předání elektronických informací a rovněž samotného zařízení klíče nebo zámku.

#### Chráněný režim

Pro vyřešení problému bezpečného dodání zařízení k, například, zákazníkovi nebo distributorovi je znakem zařízení zámku a klíče podle předkládaného vynálezu tak zvaný chráněný režim. To v podstatě znamená, že uživatelé na různých úrovních hierarchie, to jest výrobce, distributor a koncový uživatel, mají plnou kontrolu nad autorizací zařízení příslušejících k systému.

To je provedeno použitím proměnného kódovacího klíče uloženého v elektronickém kódu zařízení. Funkce tohoto proměnného kódovacího klíče bude popsána v následujícím popisu ve spojení s odkazy na obr. 5a až obr. 5e, na kterých je ilustrován obsah elektronického kódu, uloženého ve elektronické paměti zařízení.

Nejprve je vytvořen polotovár zařízení u výrobce, to jest zařízení bez mechanického nebo elektronického kódování. Paměť elektronického kódu je tudíž prázdná, viz obr. 5a.

Následujícím krokem u výrobce je přidání kódového prvku specifického pro příslušného výrobce, viz obr. 5b. Tento kódový prvek, označený „M“, identifikuje specifického výrobce a je unikátní pro každého výrobce. Je tudíž možné pouhým přečtením kódového prvku M zjistit, od kterého výrobce klíč (nebo zámek) pochází.

Prvek označený „ $K_{DES-M}$ “ je DES kódovací klíč použitý výrobcem M jako transportní nebo ukládací kód. Jak již bylo uvedeno, kódovací klíč  $K_{DES}$ , potřebný pro fungující zařízení, je přítomen pouze v zařízeních ve funkčním režimu, to jest v aktivovaných klíčích a zámcích fungujících v MKS zákazníka 100. Klíč  $K_{DES-M}$  je vytvořen softwarem výrobce (M-software) a pro nikoho vyjma výrobce majícího M-software není možné, aby vytvořil polotovár klíče (nebo zámku) s unikátním klíčem  $K_{DES-M}$  pro tohoto specifického výrobce. Tímto způsobem jsou klíče chráněny během skladování u výrobce, protože jsou nepoužitelné pro kohokoliv vyjma správného příslušného výrobce.

Když má výrobce zařízení odeslat k distributorovi, je přidán prvek elektronického kódu, specifický pro příslušného distributora, viz obr. 5c. Tento prvek, označený „D“, identifikuje specifického distributora a je unikátní pro každého distributora. Tento prvek je uložen do pozice obvykle používané MKS kódem.

Současně je u výrobce nahrazen kódovací klíč  $K_{DES-M}$  klíčem  $K_{DES-D}$ , což je kódovací klíč unikátní pro příslušného distributora. Aby ale bylo možné provést tuto změnu, musí být mezi chráněným klíčem (zařízením) výrobce a M-klíčem provedeno ověření. Tento ověřovací proces je úspěšný pouze tehdy, když kódovací klíče chráněného zařízení výrobce a M-klíče, to jest  $K_{DES-M}$ , jsou shodné. Kódovací klíč  $K_{DES-D}$  je uložen v M-software, odkud je vyjmut po úspěšném ověřovacím procesu. Opatřené kódovacím klíčem  $K_{DES-D}$  je nyní zařízení v chráněném režimu distributora.

Když je zákazníkem podána objednávka, buď výrobcí nebo distributorovi, je inicializován proces uvedení klíče (zařízení) do chráněného režimu zákazníka, jak bylo popsáno ve spojení s odkazy

na obr. 4. Potom jsou elektronicky vyslány informace potřebné pro tento proces ze softwaru výrobce k distributorovi, ale ne jako prostý text. Tyto informace jsou naopak vyslány kódované s kódovacím klíčem  $K_{DES-D}$  distributora. Například je vyslán kódovací klíč  $K_{DES-C}$  zákazníka pro zařízení v chráněném režimu zákazníka v následujícím formátu:

5

$$eK_{DES-D}(K_{DES-C})$$

Další relevantní informační prvky, jako je MKS, GR, UID,  $K_{DES}$  a, pokud není použit chráněný režim zákazníka,  $K_{DES-C}$ , jsou vyslány kódované stejným způsobem. Tyto informace jsou potom staženy do chráněného klíče (zařízení) distributora.

10

Aby se dekodovaly kódované informace, musí u distributora proběhnout ověřovací proces. Tento proces probíhá mezi chráněným zařízením a D-klíčem, ve kterém je uložen kódovací klíč  $K_{DES-D}$ . Prvky kódu jsou tudíž dekódovány, čímž je chráněné zařízení distributora, znázorněné na obr. 5c, převedeno na chráněné zařízení zákazníka, jak je znázorněno na obr. 5d. Současně je uložen správný kódový prvek funkce „F“, který indikuje funkci zařízení, například uživatelský klíč.

15

Zařízení opouštějící distributora ale ještě nemůže být použito v koncovém systému hlavního klíče zákazníka, to jest není ještě ve funkčním režimu. Prostřednictvím C-softwaru a C-klíče zákazník přijímá chráněné zařízení zákazníka a nahrazuje kódovací klíč  $K_{DES-C}$  kódovacím klíčem  $K_{DES}$ , viz obr. 5e. Teprve potom může být zařízení použito v systému hlavního klíče.

20

C-klíč je obvykle dodáván od výrobce přímo k zákazníkovi. Výraz „chráněný režim zákazníka“ vyjadřuje skutečnost, že nikdo jiný než správný autorizovaný zákazník nemůže použít klíč (zařízení) dodaný distributorem, protože klíče (zařízení) zamykacího systému musí být přijaty systémem prostřednictvím C-klíče.

25

Znak, že fyzický klíč, to jest systémový klíč, je použit pro změnu kódu dalšího zařízení, má několik výhod. Za prvé s fyzickým klíčem se snadno manipuluje. Za druhé toto uspořádání zajišťuje bezpečnost systému. Nikdo nemůže uvést zařízení do funkčního režimu bez správného systémového klíče (například C-klíče).

30

V alternativním provedení předkládaného vynálezu je vypuštěna úroveň distributora. Výrobce je tudíž odpovědný za kroky popisované ve spojení s obr. 5a až obr. 5c a dodává jak zařízení tak i systémový klíč zákazníkovi. To neovlivní bezpečnost systému, pokud zařízení a systémové klíče jsou dodávány odděleně.

35

Alternativně, pokud si to přeje zákazník, mohou být klíče k zákazníkovi dodávány ve funkčním režimu, to jest s již uloženým kódovacím klíčem  $K_{DES}$ . To by poskytovalo méně bezpečný systém, ale možnost vypustit jeden nebo několik kroků na druhou stranu ukazuje na pružnost konceptu chráněného režimu.

40

Jak již bylo uvedeno informační prvek F – prvek funkce – elektronického kódu určuje úlohu zařízení. Tento prvek je „0“, to jest nedefinovaný během skladování u výrobce nebo distributora a je mu dána předem stanovená hodnota, když je klíč (zařízení) uváděn do funkčního režimu. Tato hodnota závisí na úloze klíče (zařízení); to jest, zda je zámkem nebo uživatelského klíčem, C-klíčem, D-klíčem, nebo M-klíčem. Přesný způsob, jakým je prováděna tato identifikace, není pro předkládaný vynález důležitý.

45

50

Bezpečnost výměny dat

V následujícím budou ve spojení s odkazy na obr. 6 diskutovány bezpečnostní aspekty datové výměny mezi softwarem na různých úrovních hierarchie. Každá dvojice výrobce–distributor, výrobce zákazník a distributor–zákazník má svůj vlastní kódovací klíč za účelem zajištění posta-

55

čujícího zabezpečení. Stejně kódovací klíče jsou ale použity v obou směrech, to jest, například, jak od distributora k zákazníkovi tak i od zákazníka k distributorovi. Všechny požadované kódovací klíče jsou uloženy v příslušném softwaru. Kódovací klíče jsou dodány společně se softwarem, ale pokud kódovací klíče mají být aktualizovány, jsou od výrobce zaslány nové kódovací klíče zakódované s aktuálními komunikačními kódovacími klíči.

#### Uživatelské a systémové klíče

Každý uživatel systému, znázorněného na obr. 2, musí být identifikován použitým softwarem. K tomuto účelu má každý uživatel své vlastní unikátní uživatelské jméno a přísluší do jedné ze tří uživatelských kategorií: superuživatel, čtení/zápis, nebo pouze čtení. Různé kategorie mají různá privilegia a přístupová omezení, která budou stručně diskutována níže.

Kategorie superuživatel může měnit uživatelská práva a vlastnictví systémových klíčů. Může rovněž měnit heslo a kód PIN všech systémových klíčů a uživatelů a měnit autorizaci C-klíč v softwaru. Navíc tato kategorie může provádět všechny operace povolené uživateli v kategorii čtení/zápis. Aby získal přístup k softwaru, superuživatel potřebuje speciální systémový klíč, tak zvaný hlavní systémový klíč, a musí zadat kód PIN. Pro každý software je pouze jeden hlavní systémový klíč.

Uživatel v kategorii čtení/zápis může měnit autorizaci v zamykací mapě systému MKS. Může rovněž dekódovat a kódovat soubory pro přenos do jiného softwaru v systému. Aby získal přístup k softwaru, uživatel v kategorii čtení/zápis potřebuje autorizovaný systémový klíč a musí zadat kód PIN.

Aby získal přístup k softwaru, uživatel v kategorii pouze čtení potřebuje klíč příslušející systému MKS a potřebuje zadat heslo. Uživatel v kategorii pouze čtení může pouze číst uspořádání zamykacího systému, to znamená, že může sledovat zamykací mapu a nemůže provádět jakékoliv změny autorizací, a tak dále.

Je také vytvořen ověřovací protokol mezi uživatelem, systémovými klíči a různým softwarem. Kódovací klíč  $K_{SWDj}$  identifikace softwaru je uložen v softwaru v kódovaném souboru. Tento kódovací klíč  $K_{SWDj}$  je unikátní pro každý systémový klíč, přičemž úplný ověřovací proces sleduje následující kroky: Za prvé jsou vzájemně vyměněny veřejné identity mezi softwarem a systémovým klíčem. Uživatel potom zadá uživatelské jméno a kód PIN. Software potom ověří pravost systémového klíče podobným způsobem, jako je popsáno níže v kapitole označení „Zabezpečení databáze“, s použitím výše zmiňovaného unikátního kódovacího klíče identifikace softwaru.

#### 40 Zabezpečení databáze

V následujícím popisu budou diskutovány aspekty zabezpečení databáze ve spojení s odkazy na obr. 7 a obr. 8, které ilustrují kódování databáze, použité se systémem znázorněným na obr. 2. V jednom MKS jsou různé informační položky uloženy v různých souborech. To znamená, že pokud je kódovací klíč narušen, byla narušena pouze část databáze. Příklady různých informačních prvků jsou:

- Soubor1 – zamykací mapa
- Soubor2 – seznam klíčů a zámků s jejich veřejnou identitou (PID)
- Soubory

Každý z těchto souborů je kódován se samostatným kódovacím klíčem, které jsou ve znázorněném příkladu označeny  $K_{DB-F1}$ ,  $K_{DB-F2}$ , ...,  $K_{DB-Fi}$ , viz obr. 7.

Uživatel přistupující k softwaru bude poskytovat své uživatelské jméno a kód PIN (vyjma případu uživatele v kategorii pouze čtení, ve kterém je namísto toho zadáváno heslo). Uživatel rovněž použije systémový klíč  $j$  a je inicializován ověřovací proces. Za předpokladu úspěšného ověřovacího procesu je kódovací klíč  $K_{SYSj}$ , uložený v systémovém klíči  $j$  použit pro přístup k softwaru, použit v následujících dekódovacích procesech. Jak je patrné na obr. 7, kódovací klíč  $K_{SYSj}$  je použit při vybírání sady kódovaných kódovacích klíčů  $K_{DB-F1}$ ,  $K_{DB-F2}$ , ...,  $K_{DB-Fi}$ , a tak dále, použitých pro kódování databázových souborů 1, 2, 3, a tak dále. Kódovací klíče  $K_{DB-F1}$ ,  $K_{DB-F2}$ , ...,  $K_{DB-Fi}$ , a tak dále, jsou tedy samy uloženy kódované s kódovacím klíčem  $K_{SYSj}$  a jsou dekódovány prostřednictvím tohoto kódovacího klíče, uloženého v autorizovaném fyzickém systémovém klíči.

Za účelem přečtení, například, souboru 1 je dekódovaný kódovací klíč  $K_{DB-F1}$  použit pro dekódování informací uložených v databázi. Aby se ale dále zvýšilo zabezpečení, tento kódovací klíč souboru je modifikován pokaždé, když je přistupováno k souboru. To se provádí prostřednictvím modifikátoru  $R_{DB-i}$ , viz obr. 7 a obr. 8. Aktuální kódovací klíč, použitý pro dekódování určitého souboru, se nazývá  $K_{DB-Fi-mod} = K_{DB-Fi} + R_{DB-i}$ . Pokaždé, když je ukládán soubor  $i$ , je vypočítán nový  $R_{DB-i}$ , tento soubor  $i$  je kódován s novým  $K_{DB-Fi-mod}$  a je uložen nový  $R_{DB-i}$  v prosté podobě.

Je důležité, že používané kódovací klíče nejsou ukládány po zbytečně dlouhou časovou periodu. Jak je tedy patrné na obr. 7, datové prvky naznačené v bloku A jsou uloženy pouze v primární paměti a ne na disku. Datové prvky a informační soubory, naznačené v bloku B na obr. 7, jsou uloženy na disku. Toto řešení zajišťuje bezpečné uložení databáze klíčů, protože kódovací klíče existují v počítači pouze tak dlouho, jak dlouho je zapnutý. Tak například, pokud je počítač s databází ukraden, není zde nebezpečí, že v počítačovém systému potom budou přítomné dekódované kódovací klíče.

#### Identifikační procedura

Když je klíč zasunut do zámku, je inicializována identifikační procedura. Tato identifikační procedura je založena na použití kódovaných klíčů a je dále popsáno v souběžné patentové přihlášce SE-9901643-8, na kterou je zde učiněn odkaz. Důležitým znakem této procedury je ale to, že dvě vzájemně spolu komunikující zařízení musí mít stejný kódovací klíč, aby byl proces úspěšně proveden, jako je například ověřovací proces.

Výše byla popsána výhodná provedení předkládaného vynálezu. Osoba v oboru znalá snadno nahlédne, že zamykací zařízení podle vynálezu může být měněno, aniž by byl opuštěn rozsah vynálezu, jak je definován v připojených patentových nárocích. Tak například, zatímco byl ve spojení s výhodnými provedeními popisován DES kódovací algoritmus, stejně tak dobře mohou být použity i jiné kódovací postupy.

## PATENTOVÉ NÁROKY

5

1. Způsob autorizace uživatelského zařízení systému klíče a zámku, přičemž uživatelským zařízením je uživatelský klíč (101) nebo zámek (20) systému (100) hlavního klíče, přičemž tento způsob zahrnuje následující kroky:

- vytvoření uživatelského zařízení (UD1) majícího elektronické obvody,
- 10 – vytvoření prvního systémového zařízení (SD1) majícího elektronické obvody a používaného v první úrovni (úroveň 1) systému klíče a zámku, a
- uložení prvního kódovacího klíče v prvním uživatelském zařízení a v prvním systémovém zařízení,

**vyznačující se tím**, že zahrnuje kroky

- 15 – provedení ověřovacího procesu mezi uživatelským zařízením a prvním systémovým zařízením s použitím prvního kódovacího klíče, a
- v případě, že ověřovací proces byl úspěšný, provedení softwarové operace prvním systémovým zařízením, ve které se první kódovací klíč, uložený v uživatelském zařízení, nahradí druhým kódovacím klíčem,
- 20 – přičemž druhý kódovací klíč se uloží v druhých systémových zařízeních (SD2) a dalších uživatelských zařízeních (UD2, UD3) použitých v druhé úrovni (úroveň 2) systému klíče a zámku, čímž se dosáhne toho, že uživatelské zařízení je provozuschopné s druhými systémovými a dalšími uživatelskými zařízeními.

25 2. Způsob podle nároku 1, **vyznačující se tím**, že během kroku náhrady prvního kódovacího klíče, uloženého v uživatelském zařízení, se druhý kódovací klíč dodá prostřednictvím prvního systémového zařízení (SD1).

30 3. Způsob podle nároku 1, **vyznačující se tím**, že během kroku náhrady prvního kódovacího klíče, uloženého v uživatelském zařízení, se druhý kódovací klíč dodá prostřednictvím počítače (C1).

4. Způsob podle nároku 3, **vyznačující se tím**, že zahrnuje přídatný krok dodání druhého kódovacího klíče do počítače (C1) přes síť, jako jsou lokální síť a veřejné telefonní síť.

35

5. Způsob podle kteréhokoliv z nároků 1 až 4, **vyznačující se tím**, že prvním systémovým zařízením je systémový klíč systému hlavního klíče.

40 6. Způsob podle kteréhokoliv z nároků 1 až 5, **vyznačující se tím**, že uživatelským zařízením je uživatelský klíč (101) systému (100) hlavního klíče.

7. Způsob podle kteréhokoliv z nároků 1 až 5, **vyznačující se tím**, že uživatelským zařízením je zámek (20) systému (100) hlavního klíče.

45 8. Způsob podle kteréhokoliv z nároků 1 až 7, **vyznačující se tím**, že elektronické kódovací klíče jsou nečitelné z vnějšku uvedených elektronických obvodů.

9. Systém klíče a zámku, který zahrnuje:

- množství uživatelských zařízení (UD1 – UD3) zahrnujících:
- 50 – množství uživatelských klíčů majících elektronické obvody zahrnující elektronickou paměť upravenou pro uložení proměnného elektronického kódovacího klíče, a

- množství zámků majících elektronické obvody zahrnující elektronickou paměť upravenou pro uložení proměnného elektronického kódovacího klíče,
- přičemž uživatelský klíč a zámek jsou spolu provozuschopné pouze tehdy, když jsou v tomto uživatelském klíči a zámku uloženy shodné kódovací klíče,
- 5    **v y z n a č u j í c í   s e   t í m ,   ž e   z a h r n u j e**
  - alespoň jedno systémové zařízení (SD1 až SD3) mající elektronické obvody zahrnující elektronickou paměť upravenou pro uložení trvalého elektronického kódovacího klíče, a
  - počítačový programový software upravený pro změnu proměnného elektronického kódovacího klíče uživatelského zařízení z prvního kódovacího klíče na druhý kódovací klíč v důsledku
  - 10    úspěšného ověřovacího procesu provedeného mezi
    - zámkem nebo uživatelským klíčem, majícím uložený proměnný elektronický kódovací klíč,
    - a
    - systémovým zařízením majícím shodný kódovací klíč jako uvedený zámek nebo uživatelský klíč,
  - 15    – přičemž druhý kódovací klíč je uložen v druhých systémových zařízeních (SD2) a uživatelských zařízeních (UD2, UD3), používaných v druhé úrovni (úroveň 2) systému klíče a zámku, čímž jsou uživatelská zařízení provozuschopná s těmito druhými systémovými a uživatelskými zařízeními.

20

7 výkresů

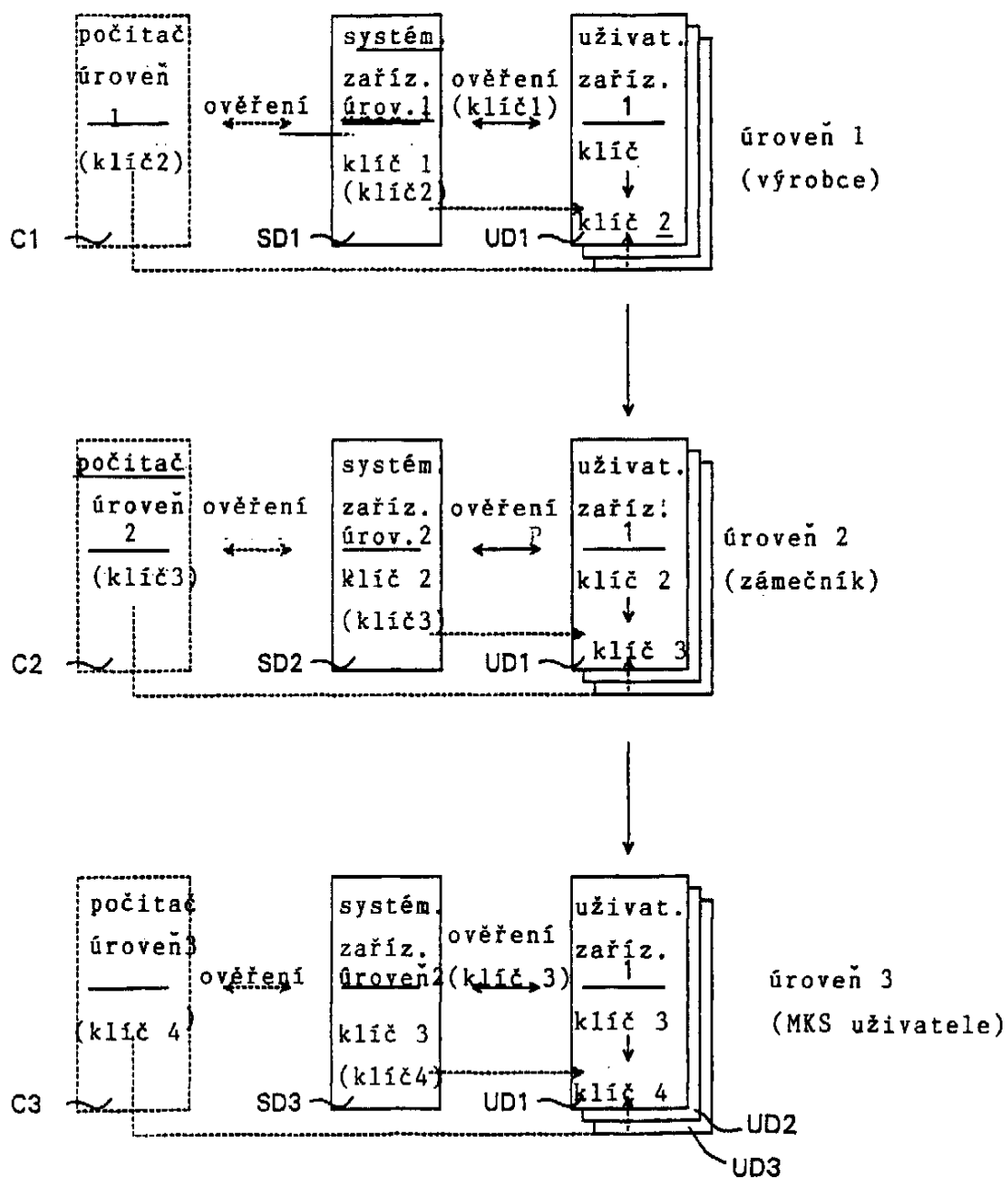


Fig. 1

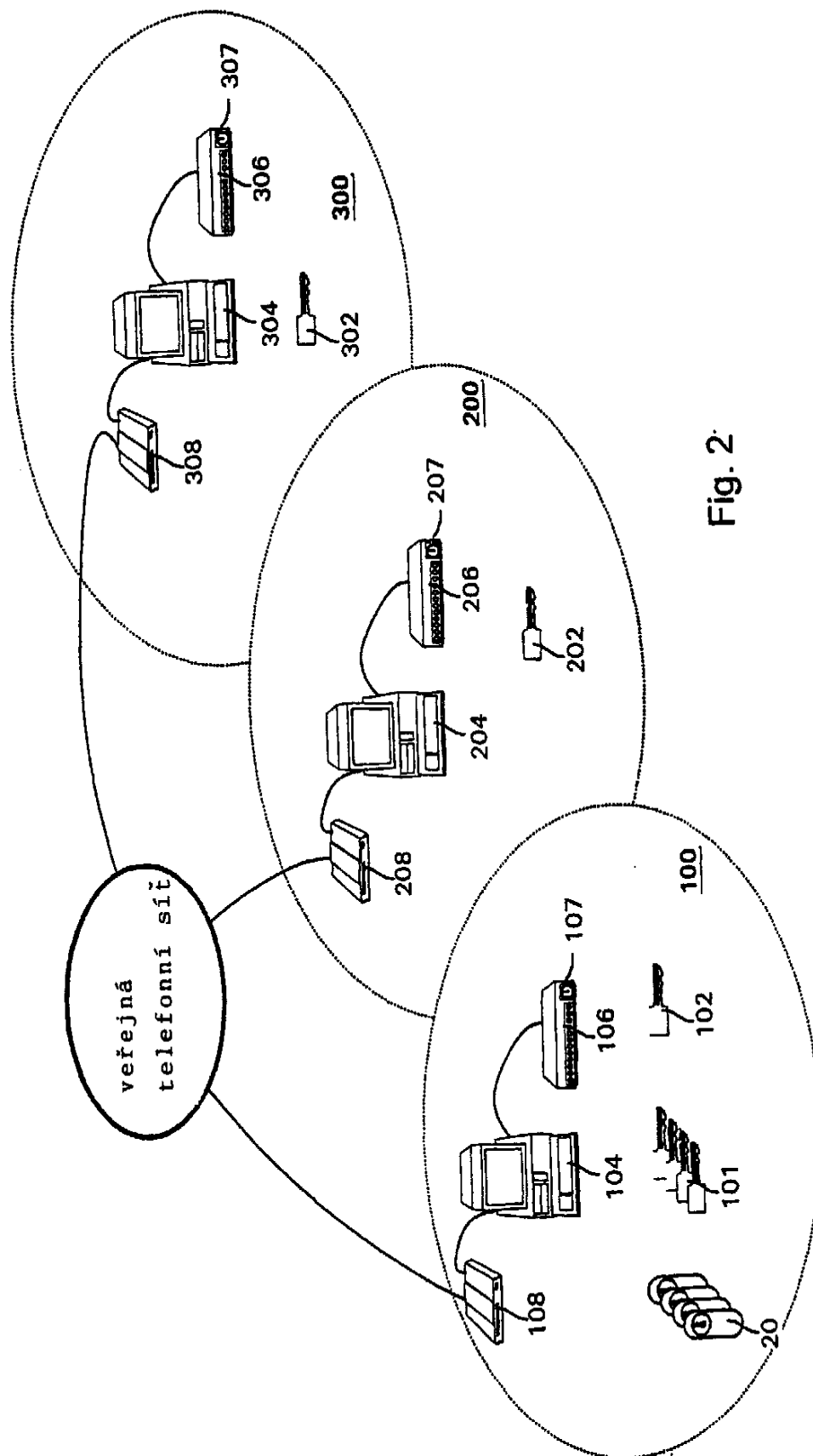


Fig. 2

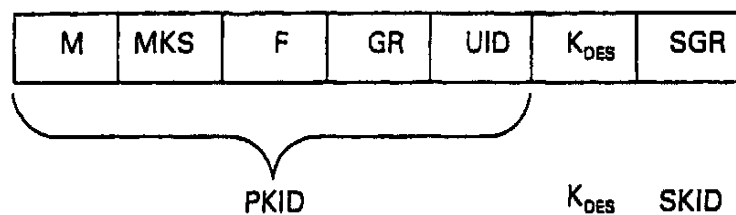


Fig. 3a

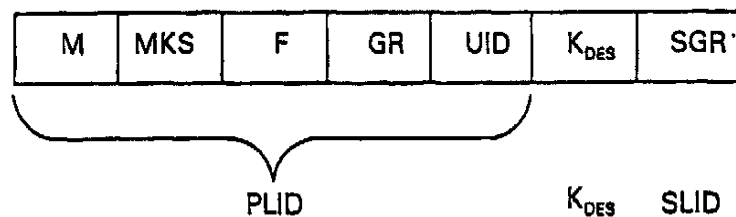


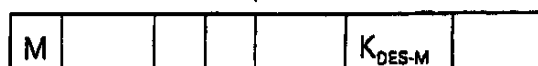
Fig. 3b

Fig. 5a



M-software

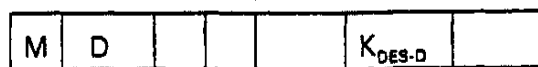
Fig. 5b



M-software

M-klíč

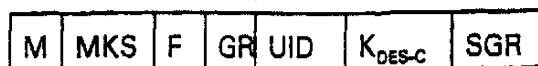
Fig. 5c



D-software

D-klíč

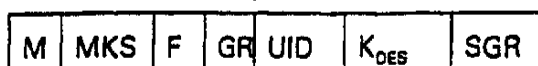
Fig. 5d



C-software

C-klíč

Fig. 5e



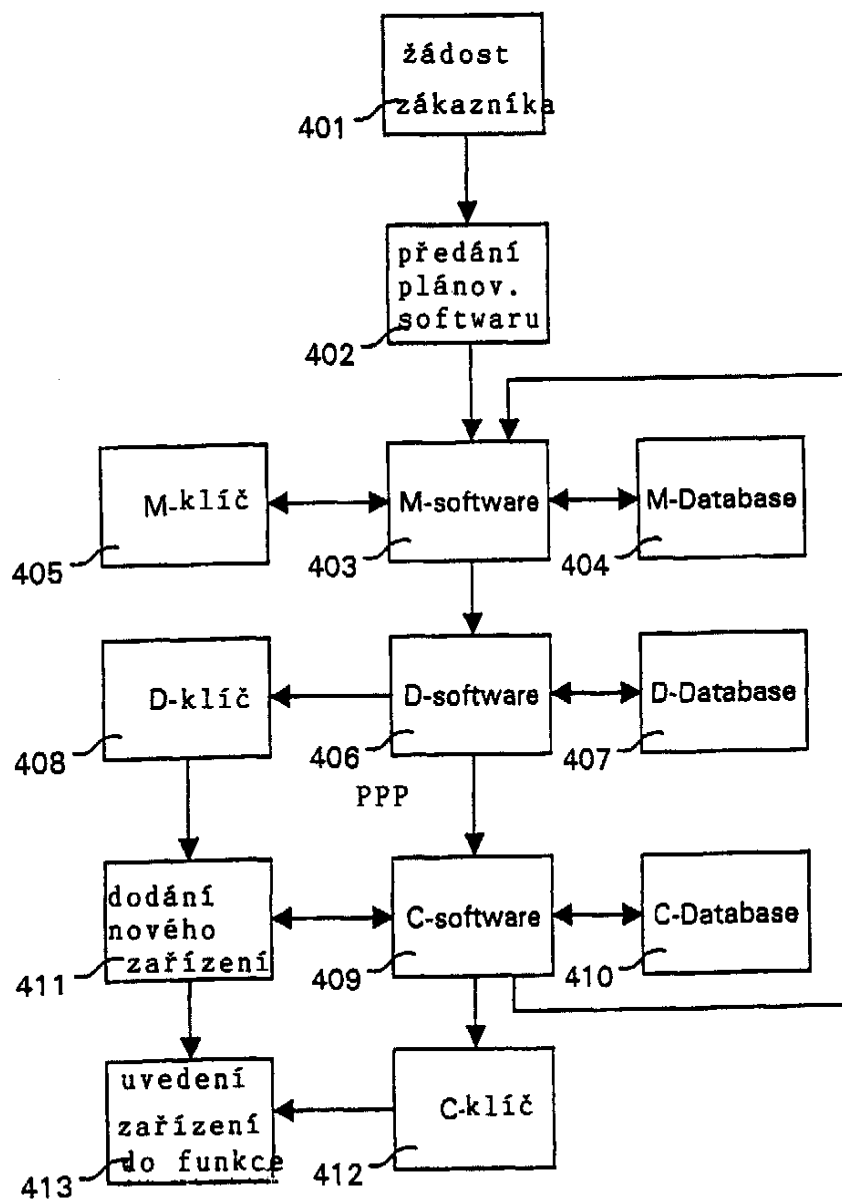


Fig. 4

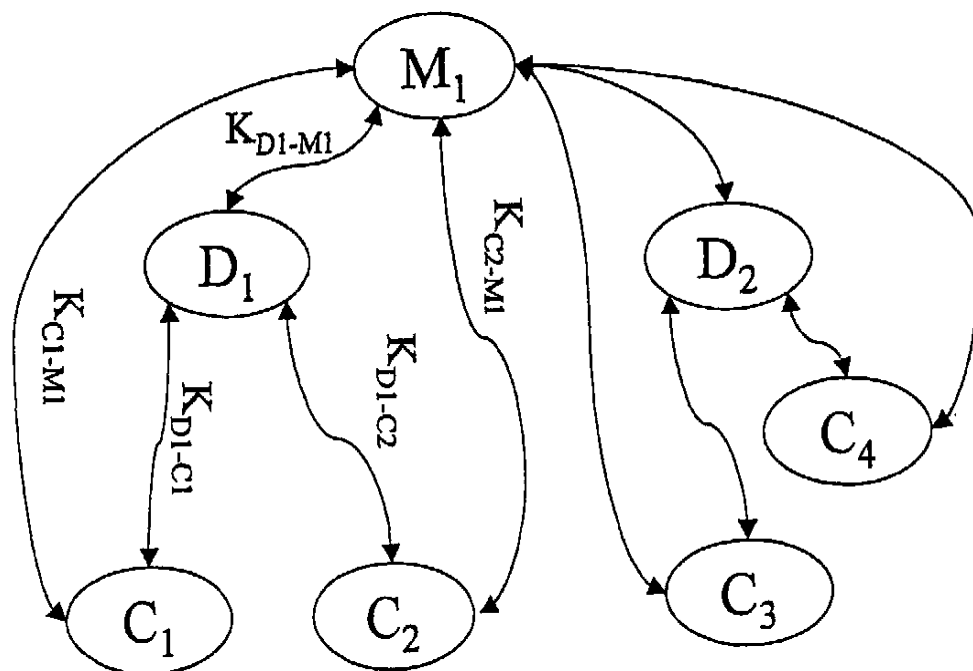
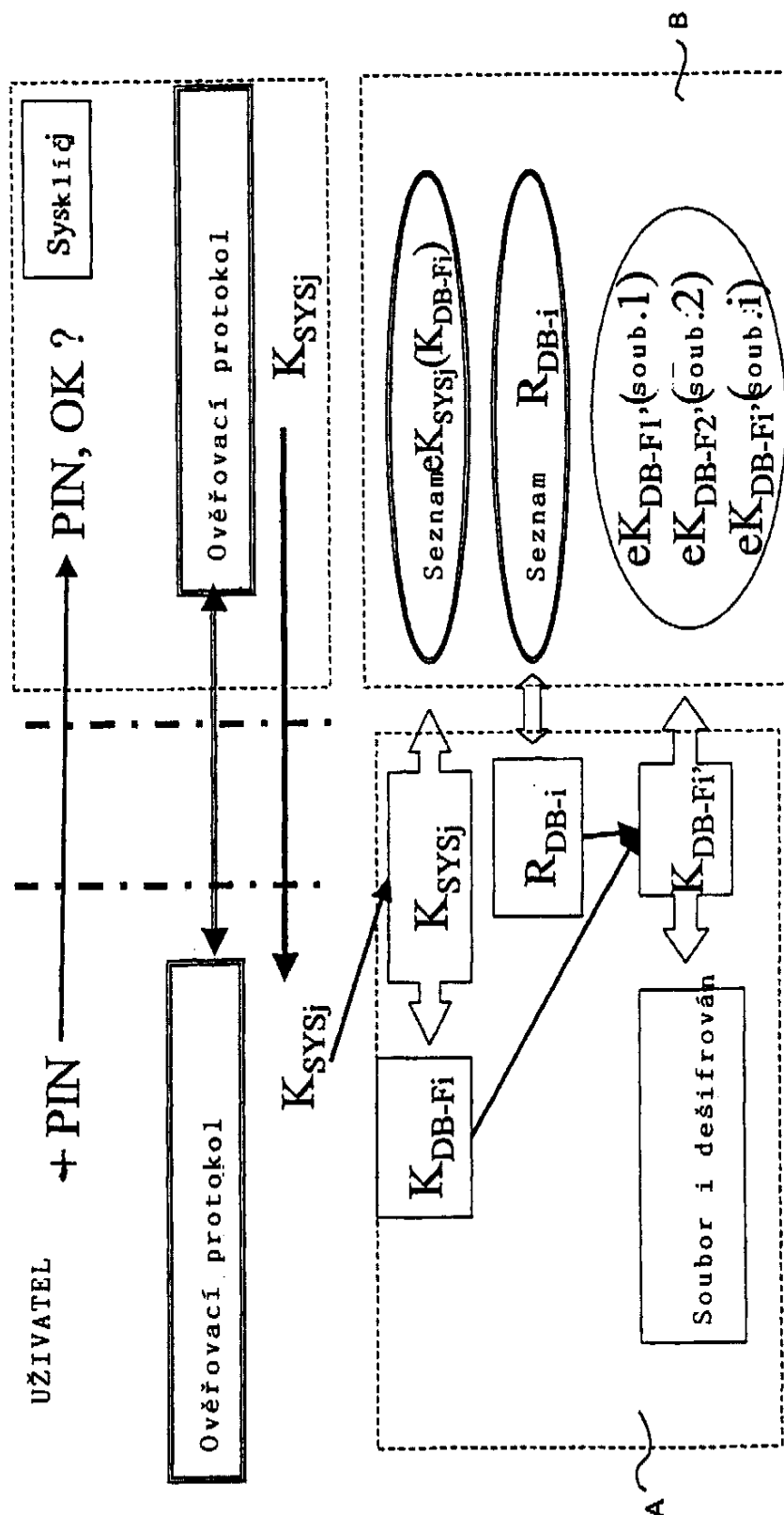


Fig. 6



**Fig. 7**

|              | $DB_{\text{soub}1}$     | $DB_{\text{soub}2}$     | ... | $DB_{\text{soub}j}$     |
|--------------|-------------------------|-------------------------|-----|-------------------------|
| $Sys_{*1i1}$ | $eeK_{SYS1}(K_{DB-F1})$ | $eeK_{SYS1}(K_{DB-F2})$ | ... | $eeK_{SYS1}(K_{DB-Fi})$ |
| $Sys_{*1i2}$ | $eeK_{SYS2}(K_{DB-F1})$ | $eeK_{SYS2}(K_{DB-F2})$ | ... | $eeK_{SYS2}(K_{DB-Fi})$ |
| ...          | ...                     | ...                     | ... | ...                     |
| $Sys_{*1ij}$ | $eeK_{SYSj}(K_{DB-F1})$ | $eeK_{SYSj}(K_{DB-F2})$ | ... | $eeK_{SYSj}(K_{DB-Fi})$ |

|                    |                     |                     |
|--------------------|---------------------|---------------------|
| $DB_{\text{soub}}$ | $DB_{\text{soub}2}$ | $DB_{\text{soub}j}$ |
| $R_{DB-F1}$        | $R_{DB-F2}$         | $R_{DB-Fi}$         |

Fig. 8

Konec dokumentu