

**УКРАЇНА****(19) UA****(11) 106642****(13) C2****(51) МПК****H04W 12/08** (2009.01)**H04W 12/06** (2009.01)**H04W 12/04** (2009.01)

**ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ**

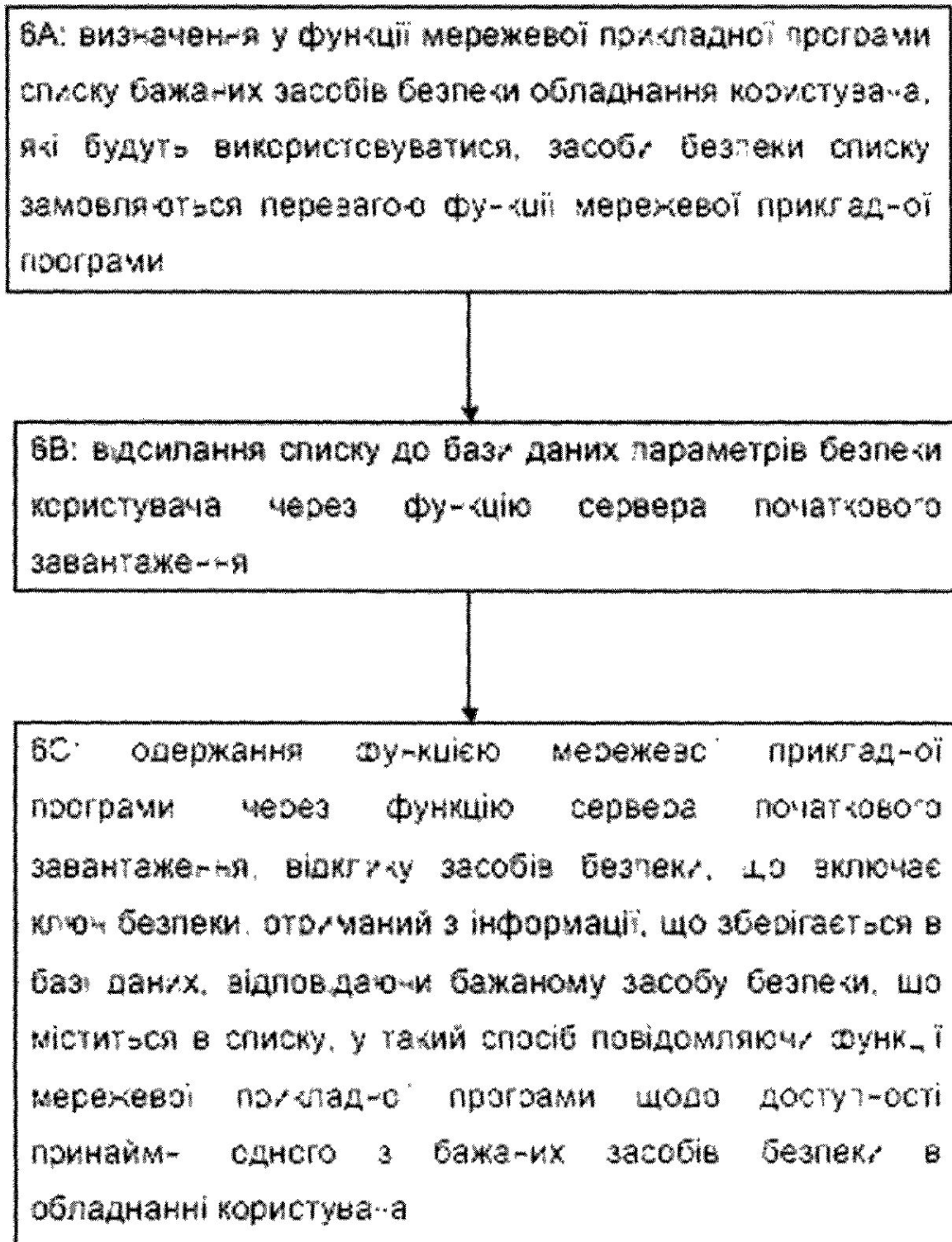
(12) ОПИС ДО ПАТЕНТУ НА ВІНАХІД

(21) Номер заявки:	а 2012 08486	(72) Винахідник(и):	Гольтманнс Зільке (FI)
(22) Дата подання заявки:	22.11.2010	(73) Власник(и):	НОКІА КОРПОРЕЙШН,
(24) Дата, з якої є чинними права на винахід:	25.09.2014		Keilalahdentie 4, FI-02150 Espoo, Finland (FI)
(31) Номер попередньої заявки відповідно до Паризької конвенції:	61/284,045	(74) Представник:	Крилова Надія Іванівна, реєстр. №30
(32) Дата подання попередньої заявки відповідно до Паризької конвенції:	11.12.2009	(56) Перелік документів, взятих до уваги експертизою:	US 2006205388 A1; 14.09.2006 US 2007101122 A1; 03.05.2007 WO 2008084135 A1; 17.07.2008
(33) Код держави-учасниці Паризької конвенції, до якої подано попередню заяву:	US		
(41) Публікація відомостей про заяву:	10.10.2012, Бюл.№ 19		
(46) Публікація відомостей про видачу патенту:	25.09.2014, Бюл.№ 18		
(86) Номер та дата подання міжнародної заявки, поданої відповідно до Договору РСТ	РСТ/FI2010/050944, 22.11.2010		

(54) ПРОФІЛЬ ЗАСОБУ БЕЗПЕКИ СМАРТ-КАРТКИ У СЕРВЕРІ АБОНЕНТСЬКИХ ДАНИХ**(57) Реферат:**

Відповідно до типових втілень винаходу є принаймні метод, здійснення комп'ютерна програма та обладнання для того, щоб визначати у функції мережевої прикладної програми список бажаних засобів безпеки обладнання користувача, які будуть використовуватися, засоби безпеки списку замовляються перевагою функції мережевої прикладної програми, відіслати список до бази даних параметрів безпеки користувача через функцію сервера початкового завантаження та одержувати функцією мережевої прикладної програми, через функцію сервера початкового завантаження, відклик засобів безпеки, що включає ключ безпеки, отриманий з інформації, що зберігається в базі даних, відповідаючи бажаному засобу безпеки, що міститься в списку, у такий спосіб повідомляючи функції мережевої прикладної програми щодо доступності принаймні одного з бажаних засобів безпеки в обладнанні користувача.

UA 106642 C2



Фіг.6

[0001] Ця заявка на патент вимагає пріоритет відповідно до 35 Зводу Законів США (U.S.C), § 119 (e), Тимчасової Заявки на патент №61/284,045, поданої 11 грудня 2009 року, розкриття якої повністю включається посиланням в цьому документі.

Технічна галузь:

5 [0002] Ідеї відповідно до типових та необмежуваних втілень даного винаходу відносяться взагалі до систем бездротових комунікацій, методів, пристроїв та комп'ютерних програм, та, більш конкретно, стосуються загальної архітектури початкового завантаження та до засобів безпеки.

Передпосилки створення винаходу:

10 [0003] Цей розділ призначений, щоб забезпечити історію питання або обставини винаходу, що викладено у формулі винаходу. Опис в цьому документі може включати поняття, які могли розглядатися, але не обов'язково є поняттями, які були раніше зрозумілі, здійснені або описані. Тому, якщо інакше не зазначене в цьому документі, те, що описується в цьому розділі, не є відомим рівнем техніки щодо опису та формули винаходу у цій заявці та не береться до

15 відомого рівня техніки включенням у цей розділ.

[0004] Наступні скорочення, які можуть бути знайдені у детальному викладенні та/або рисунках, визначаються наступним чином:

AAA аутентифікація, забезпечення (права) доступу та облік дій користувача

AKA угода щодо аутентифікації та ключу

20 AUTN ознака аутентифікації

AV вектор аутентифікації

AVP пара атрибут-значення у повідомленнях протоколу Diameter

BSF функція початкового завантаження серверу

C конфіденційний ключ

25 GAA загальна архітектура аутентифікації

GBA загальна архітектура початкового завантаження

GPL загальний рівень проштовхування

GSID GAA ідентифікатор сервісу

GUSS GBA параметри налаштування безпеки користувача

30 HLR реєстр місця розташування дому

HSS сервер абонентських даних

IK ключ цілісності

IMS підсистема передання мультимедійних даних на базі протоколу Інтернет (IP)

LDAP спрощений протокол доступу до мережевого каталогу

35 NAF мережева прикладна функція (сервіс)

NDS безпека мережевого домену

RAND випадковий запит

SLF функція вказування абонента

TLS протокол захисту (безпеки) транспортного рівня

40 UE користувацький термінал зі смарт-картою

UICC універсальна смарт-карта

uss параметри безпеки користувача

Ua UE-NAF інтерфейс для прикладних програм GAA

Ub UE-BSF інтерфейс для початкового завантаження

45 XRES відклик, що очікується при аутентифікації

Zh BSF-HSS інтерфейс для процедури початкового завантаження

Zh' BSF-HLR інтерфейс для процедури початкового завантаження

Zn BSF-NAF інтерфейс для прикладних програм GAA

Zpn NAF-BSF інтерфейс для прикладних програм GAA

50 [0005] Посилання можуть бути зроблені на наступні дві публікації:

3 GPP TS 29.109 V9.0.0 (2009-09) Технічна Специфікація Проекту Партнерства 3-го Покоління;

Технічна Специфікація Групи Базової Мережі та Терміналів; Загальна Архітектура Аутентифікації (GAA); Інтерфейси Zh та Zn, засновані на протоколі Diameter; Стадія 3 (Випуск 9); та

55 3 GPP TS 33.224 V9.0.0 (2009-09) Технічна Специфікація Проекту Партнерства 3-го Покоління; Технічна Специфікація Групи Послуг та Системних Аспектів; Загальна Архітектура Аутентифікації (GAA); Загальна Архітектура Початкового Завантаження (GBA) Рівня Простовхування (Випуск 9).

[0006] У мобільних пристроях використання GBA дозволяє аутентифікацію користувача або абонента. Використання GBA припускає, що користувач має достовірний ідентифікатор до HLR або HSS. Аутентифікацію користувача піддають обробці із використанням спільного ключа, одного у смарт-карті в мобільному пристрої для мобільних мереж, та іншого у HLR/HSS. У різних мережевих архітектурах наприклад, відокремленій мережі, спільний ключ може зберігатися в захищеному модулі (наприклад, захищеному чипі на PC), а в мережі - в сервері AAA. GBA аутентифікує користувача, маючи виклик смарт-карти мережевим компонентом та потім перевіряючи, що відповідь на виклик подібна до відповіді, передбаченої HLR/HSS, що використовує протокол AKA. BSF установлює додатковий мандат (так званий Ks). Від цього мандату він одержує індивідуальні спільні ключі постачальника послуг між об'єктом, що проходить аутентифікацію та постачальником послуг. При роботі ключ у смарт-карті використовується, щоб підтвердити приналежність до мережі. Тоді BSF одержує майстер ключ та від нього індивідуально-сервісні ключі. Термінал одержує ті ж самі ключі. В такий спосіб кожен сервіс має різні ключі (якщо один скомпрометований (відбулося несанкціоноване розкриття або втрата захищеної інформації, прим, перекладача), це стосується тільки одного сервісу). Індивідуальний спільний ключ сервісу є обмеженим у часі та для специфічного сервісного домену (що називається Ks_(ext/int)_NAF). SLF є функцією, яка повідомляє BSF, на якому HSS знайти дані абонента, у випадку коли в оператора мережі є кілька HSS.

[0007] Одна проблема, яка існує у цей час в GBA, стосується ситуації, яка виникає, коли сервіс (NAF) прагне встановити безпечне з'єднання із об'єктом, що проходить аутентифікацію у UE, особливо смарт-карті. Щоб це відбулося, NAF повинен знати, що засоби безпеки підтримуються для встановлення безпечного з'єднання. У цей час в сервісі, що забезпечує NAF, немає ніяких засобів одержати цю інформацію з терміналу або з мережі. Можна відзначити, що NAF може перебувати поза мережею оператора та, як результат, не буде мати прямого інтерфейсу до HSS.

Резюме:

[0008] У типовому аспекті винаходу є метод, що включає визначення у функції мережевої прикладної програми списку бажаних засобів безпеки обладнання користувача, які будуть використовуватися, засоби безпеки списку замовляються перевагою функції мережевої прикладної програми, відсилання списку до бази даних параметрів безпеки користувача через функцію сервера початкового завантаження, та одержання функцією мережевої прикладної програми, через функцію сервера початкового завантаження, відклику засобів безпеки, що включає ключ безпеки, одержаний з інформації, що зберігається в базі даних, що відповідає бажаному засобу безпеки, що міститься у списку, у такий спосіб інформуючи мережеву прикладну функцію щодо доступності принаймні одного з бажаних засобів безпеки в обладнанні користувача.

[0009] В іншому типовому аспекті винаходу є стійкий комп'ютерний програмоносій, що містить у собі команди комп'ютерної програми, команди комп'ютерної програми виконуються принаймні одним процесором, щоб виконати операції, що включають визначення у функції мережевої прикладної програми списку бажаних засобів безпеки обладнання користувача, що буде використовуватися, засоби безпеки списку замовляються перевагою функції мережевої прикладної програми, відсилання списку до бази даних параметрів безпеки користувача через функцію сервера початкового завантаження, та одержування функцією мережевої прикладної програми, через функцію сервера початкового завантаження, відклик засобів безпеки, що включає ключ безпеки, одержаний з інформації, що зберігається в базі даних, відповідно до бажаного засобу безпеки, що міститься в списку, у такий спосіб повідомляючи функції мережевої прикладної програми щодо доступності принаймні одного з бажаних засобів безпеки в обладнанні користувача.

[0010] У ще іншому типовому аспекті винаходу є обладнання, що включає принаймні один процесор; та принаймні один запам'ятовуючий пристрій, що містить код комп'ютерної програми, де принаймні один запам'ятовуючий пристрій та код комп'ютерної програми зконфігуровані принаймні із одним процесором, щоб змушувати обладнання принаймні визначати, у функції мережевої прикладної програми, список бажаних засобів безпеки обладнання користувача, які будуть використовуватися, засоби безпеки списку замовляються перевагою функції мережевої прикладної програми, відсилати список у базу даних параметрів безпеки користувача через функцію сервера початкового завантаження, та одержувати функцією мережевої прикладної програми, через функцію сервера початкового завантаження, відклик засобів безпеки, що включає ключ безпеки, отриманий з інформації, що зберігається в базі даних, відповідно до бажаного засобу безпеки, що міститься у списку, у такий спосіб повідомляючи функції

мережевої прикладної програми щодо доступності принаймні одного з бажаних засобів безпеки в обладнанні користувача.

Короткий опис рисунків:

[0011] Вищезгадані та інші аспекти втілень даного винаходу стають більш очевидними в наступному Детальному Описі, якщо читати у поєднанні із приєднаними Фігурами, де:

[0012] Фігура 1 - блок-схема архітектури проштовхування GBA.

[0013] Фігура 2 - блок-схема архітектури GBA.

[0014] Фігура 3 - блок-схема іншого втілення архітектури GBA.

[0015] Фігури 4A та 4B - спрощені блок-схеми UE та BSF/HSS/NAF, показаних, відповідно, на Фігурах 1-3.

[0016] Фігура 5 - схема послідовності операцій сигнал/повідомлення відповідно до типових втілень даного винаходу.

[0017] Фігура 6 - логічна схема послідовності операцій, яка ілюструє роботу методу, та результат виконання команд комп'ютерної програми, втілених у зчитуваному комп'ютером запам'ятовуючому пристрої, відповідно до типових втілень даного винаходу.

Детальний опис:

[0018] Типові втілення даного винаходу забезпечують вдосконалення для HSS, BSF та NAF.

[0019] Фігура 1 показує блок-схему архітектури Проштовхування GBA. Показані BSF 10, SLF 12, HSS 14, NAF 16 та UE 18. Ці блоки взаємно зв'язуються через інтерфейси, відзначені вище. Фігура 2 показує блок-схему архітектури GBA. На додаток до блоків, показаних на фігурі 1, база даних GUSS (DB) 20 показана як частина HSS 14. Фігура 3 - інше втілення архітектури GBA, де DB GUSS 20, як передбачається, є зовнішньою до мережі, та зв'язується з BSF 10 через деякий відповідний інтерфейс 21.

[0020] Фігура 4A показує спрощену блок-схему втілення UE 18. З метою опису типового втілення даного винаходу UE 18, як може передбачатися, включає контролер, такий як принаймні один комп'ютер або процесор даних (DP) 18A, комп'ютерно-зчитуваний запам'ятовуючий носій, втілений як принаймні один запам'ятовуючий пристрій (MEM) 18B, який зберігає програму машинних команд (PROG) 18C, та принаймні один відповідний трансивер, такий як радіочастотний (RF) трансивер 18D, для двобічних (наприклад, бездротових) комунікацій з BSF 10 та NAF 16 через один або більш проміжних вузлів, таких як одна або базова станції, перетворюючи вузли або модулі доступу (не показано). UE 18, як передбачається, включає смарт-карту або захищений модуль 18E для обробки безпечного мандата, що виконаний у запам'ятовуючому пристрої та іншими функціональними можливостями. Загалом, ця функція може бути включена в карту, таку як змінна карта, або в безпечному (захищеному) чипі або модулі (не обов'язково карті). Смарт-карта або захищений модуль 18E можуть включати, або можуть бути втілені в або з, модулем ідентичності абонента (SIM).

[0021] Смарт-карта або захищений модуль 18E може також згадуватися як UICC. Як відомо, UICC - смарт-карта, що використовується в мобільних терміналах у мережах GSM та UMTS, але вона також може бути виконана у різному формфакторі, наприклад, на захищеному чипі апаратного обладнання. UICC гарантує безпеку взаємодії між пристроєм користувача (мобільний телефон, PC, смарт-карта) та мережею. У мережі GSM смарт-карта є SIM-картою. UICC може містити застосування SIM, у мережі UMTS, вона містить застосування USIM та для мереж IMS - застосування ISIM. UICC може містити кілька застосувань паралельно, дозволяючи тієї ж самій смарт-карті надати доступ як до мережі GSM так і до мережі UMTS та інших застосувань (наприклад, мобільні банківські операції, підтримка Мобільного телебачення, та т. ін.). У мережі CDMA UICC містить застосування CSIM, на додаток до 3GPP USIM та SIM застосувань.

[0022] Фігура 4B показує спрощену блок-схему втілення обладнання, що може використовуватися для здійснення одного або всіх з BSF 10, HSS 14 та NAF 16. В основному, ці компоненти можуть бути розглянуті як комп'ютерна система, що має, наприклад, у випадку BSF 10, контролер, такий як принаймні один комп'ютер або процесор даних (DP) 10A, комп'ютерно-зчитуваний запам'ятовуючий носій, втілений як принаймні один запам'ятовуючий пристрій (MEM) 10B, який зберігає програму машинних команд (PROG) 10C, та принаймні один відповідний трансивер для двобічних комунікацій через певні інтерфейси (Zh, Zn, Zpn, Ub, Dz) з іншими компонентами архітектури GBA. Є додаткові інтерфейси для випадку використання модулю доступу або використання HLR. Але ці додаткові інтерфейси показані на рисунку 4B.

[0023] Раніше в 3GPP було погоджено, що інформація, що стосується того чи підтримує UE смарт-карта 18E встановлення безпечного з'єднання, повинна зберігатися в HSS GUSS 20. Це було задокументовано у 3 GPP TS 33.224, як "Здатності GPL U повинні бути збережені у GUSS

у HSS." Однак, механізм, потік повідомлень та обробка не були визначені для того, як ця запропонована функціональність буде втілена, здійснена та приведена у дію.

[0024] Використання типових втілень даного винаходу дозволяє використання смарт-карти, або більш широко, специфічного засобу безпеки або прикладної програми постачальника послуг, коли постачальник послуг в змозі указати, яка функція смарт-карти 18E (тобто, який специфічний засіб безпеки або прикладної програми) повинен бути використаний, так само як ідентифікувати засіб другого вибору ("майже найкращий").

[0025] Відповідно до типових втілень між сервісом та вузлом генерації ключа (BSF 10) та між BSF 10 та HSS 14 поширюються повідомлення. Зберігання інформації про безпеку користувача в HSS 14 також поширюється, та HSS 14 опрацьовує цю додаткову інформацію. BSF 10, як очікують, буде враховувати показання, що надаються HSS 14.

[0026] Кінцевий результат полягає в тому, що сервіс знає, який засіб може бути використаний, спілкуючись із UE 18 та в такий спосіб у стані встановити бажане безпечне з'єднання.

[0027] Ця особливість особливо вигідна, коли, наприклад та розглядаючи більш конкретний випадок особливого інтересу типового втілення даного винаходу, NAF 16 прагне встановити безпечну сесію, використовуючи GPL зі смарт-картою 18. Однією причиною зробити це є, наприклад, мета ініціалізації.

[0028] Типові втілення даного винаходу забезпечують вдосконалення GUSS 20 та пов'язаних компонентів GBA.

[0029] Тепер посилання робиться до схеми послідовності операцій сигнал/повідомлення Фігури 5.

[0030] (1) Припускаємо, що NAF 16 прагне використовувати специфічний засіб безпеки (або застосування), такий як GPL U. NAF 16 може бути готовий "понизити", якщо цей засіб не доступний або обмежений використанням сервісу (наприклад, поріг для значення завантаження нижче, тому що рівень безпеки нижчий). Ця здатність використовувати інший резервний засіб може бути корисною в ослабленні сигнального навантаження, коли перший бажаний засіб не доступний. У цьому прикладі, припускаємо, що перший бажаний засіб є GPL U, другим бажаним засобом буде GPL з GBA U, та третім бажаним засобом буде GPL з GBA, розділені знаком ";", що дозволить вузлу одержання визначити, що починається наступне "слово". Елемент може з'явитися кілька раз для декількох засобів. Наприклад, NAF 16 бажає використовувати кілька засобів безпеки та дає список установа пріоритетів для кожного з них (наприклад, {feature1; feature2;...; feature_n}).

[0031] Таким чином, один типовий аспект винаходу - здатність указати бажаний засіб безпеки, з можливістю забезпечити список, що задає пріоритети бажаних засобів безпеки.

[0032] (2) NAF 16 указує до BSF 10, що NAF 16 бажає використовувати специфічний засіб безпеки (наприклад, GPL U). Це може бути досягнуте, додаючи поле до існуючих повідомлень Zn/Zn'. Zn визначається для Diameter та Веб-сервісу, заснованому на 3 GPP TS 29.109. Zn' є інтерфейсом для випадку, де є модуль доступу між BSF 10 та NAF 16. BSF 10 відсилає цей запит по опорній точці Zh до HSS 14. Це може бути досягнуте, додаючи поле до повідомлення запиту Zh. У випадку, де використовується HLR, BSF 10 може послати це в локальну базу даних, яка зберігає GUSS 20, та використовувати інтерфейс Zh' як є. У цьому випадку запит не є частиною стандарту, та може бути виконаний, використовуючи запит LDAP.

[0033] У типовому аспекті винаходу запит від NAF може бути GBA-Push-Info (GPI), для NAF особливий ключовий матеріал відповідає користувацькій ідентичності. Крім того, запит може використовувати протокольні інтерфейси Zpn та Zpn', наприклад як визначено у 3 GPP TS 33.223. Протокол ZPN, що є між NAF та BSF та запитом, може включати, наприклад, ідентифікатор користувача, NAF-Id, та/або GSID. Додатково, поле для елемента Запиту Засобів Безпеки може читатися як "element name="securityfeaturesrequest" type="xsd:string" minOccurs="0". NAF може запитувати інформацію про доступність засобів безпеки, використовуючи елемент Запиту Засобів Безпеки або параметр. Елемент може містити відділений крапкою із комою список засобів безпеки, які є доступні, замовлений перевагою. Відповідно до втілень, NAF може запитувати інформацію про доступність засобів безпеки, використовуючи Запит Засобу Безпеки AVP. Крім того, AVP може включати 3 GPP AV = [RAND, AUTN, XRES, CK, IK]. Запит Засобу Безпеки AVP може мати тип OctetString. AVP може містити один або декілька з засобів безпеки, які вимагає NAF.

[0034] Якщо BSF та NAF розташовуються в межах мережі того ж самого оператора, то DIAMETER, що базується на опорній точці Zpn, може бути захищений відповідно до NDS/IP. Беручи до уваги, що, якщо BSF та NAF розташовуються в мережах різних операторів,

DIAMETER, що базується на опорній точці Zpn' між Zn-Proxy та BSF може бути захищений, використовуючи TLS.

[0035] Таким чином, інший типовий аспект винаходу - здатність вдосконалювати Zn/Zn', Zpn/Zpn', та Zh з ознакою (ознаками) засобу безпеки.

5 [0036] (3) До GUSS 20 може бути додане нове поле (не у полі BSF, тому що воно буде відібране). Одне типове місце для поля, що містить новий елемент, яке буде додане, перебуває у ussType complexType, наприклад, можна додати "Засоби-UICC" або, більш широко, поле підтримки "Засоби-Безпеки". Якщо HSS 14 одержує список NAF-ініційованих, розташованих по пріоритетах засобів від BSF 10, це тоді заповнює поле підтримки Засоби-Безпеки із наданим засобом(ами). Якщо є відповідним, поле може також установити поле вибору ключа (keychoice field) UICC так, щоб BSF 10 одержав правильний прикладний специфічний ключ, наприклад Ks int NAF.a

10 [0037] У типовому аспекті винаходу, якщо BSF підтримує використання засобу безпеки та NAF запросив засіб безпеки від BSF, BSF може витягти елемент засобів безпеки від елемента bsfInfo у GUSS абонента та додати ті засоби безпеки до елемента Відклик Засобів Безпеки у відклик, що поширено в отриманому запиті Засобів Безпеки від NAF та витягнутої інформації від елемента bsfInfo. Значення додаткового елемента "securityFeatures" в елементі "bsfInfo" означає список специфічних засобів безпеки користувача, що підтримує обладнання користувача. Якщо елемент Засобу Безпеки відсутній, тоді засоби безпеки не визначені, та якщо є список декількох значень, вони відділяються ";".

20 [0038] Засоби загальної безпеки можуть бути додані до елемента Відклик Засобів Безпеки у порядку як вони з'являються в елементі bsfInfo. Якщо елемент Засоби Безпеки не визначений в GUSS, або немає ніякого засобу загальної безпеки, то BSF повинен додати порожню строку до елемента Відклик Засобів Безпеки у відклик.

25 Відклик Засобу Безпеки AVP може мати тип OctetString. AVP містить один або декілька з засобів безпеки, ідентифікованих HSS. Ця інформація може бути передана BSF із використанням елемента Засоби Безпеки, такого як в "bsfElement" GUSS, та Засоби Безпеки, отриманих у запиті. Додатково, поле для елемента Відклик Засобів Безпеки може читатися, наприклад, як "element name="securityfeaturesresponse" type="xsd:string" minOccurs="0"

30 [0039] Таким чином, інший типовий аспект винаходу - принаймні, здатність обробити список бажаного засобу (ів) в HSS 14 та BSF 10.

[0040] У цьому відношенні відмітимо, що BSF 10 може тільки одержати один ключ, хоча є в рамках цих типових втілень для BSF 10, щоб одержувати більше ніж один (наприклад, він може одержувати ключ для кожного засобу, який з'являється в розташованому по пріоритетах списку, якщо засіб підтримується).

35 [0041] (4) NAF 16 тоді одержує отриманий від BSF 10 специфічний ключ(и) сервісу та додатково одержує знання того, який рівень безпеки, можливий для комунікації між NAF 16, отримано, та який засіб(и) смарт-карти 18E NAF 16 може використовувати. BSF 10 одержує GUSS та посилає частину GUSS, тобто, USS до NAF 16. Цей USS буде містити інформацію про засіб безпеки, яку вимагає NAF 16.

[0042] Таким чином, інший типовий аспект винаходу - включення додаткової інформації, яку можна передати через поля такі як у будь-якому Zn/Zn', Zpn/Zpn', та Zh, та обробка цієї інформації в BSF 10 та NAF 16.

45 [0043] Типові втілення також охоплюють випадок, де HLR використовується замість HSS 14, та де GUSS 20 зберігається на деякій спеціалізованій зовнішній базі даних (наприклад, як на фігурі 3), так, щоб BSF 10 просто зробив виклик щоб викликати зовнішній GUSS.

[0044] Типові втілення також охоплюють випадок, де засобу безпеки інтересу не є частиною смарт-карти 18E. Наприклад, засоби безпеки можуть бути частиною захищеного чипу (наприклад, платіжне застосування, що міститься у захищеному чипі).

50 [0045] Базуючись на вищезгаданому, повинне бути очевидно, що типові втілення даного Винаходу забезпечують метод, обладнання та комп'ютерну програму(и) для вдосконалення роботи архітектури GBA, щоб подолати притаманну нестачу визначеного профілю GBA-смарт-карта в існуючому GBA або, більш загально, нестачу профілю засобу безпеки, та крім того в такий спосіб уникнути необхідності визначати та підтримувати інтерфейс нової смарт-карти терміналу (профіль засобу безпеки), щоб досягти тих же самих цілей.

55 [0046] Фігура 6 - логічна схема послідовності операцій, яка ілюструє роботу методу, та результат виконання команд комп'ютерної програми, відповідно до типових втілень даного винаходу. Відповідно до цих типових втілень метод виконує, у Блоці 6A, етап визначення у функції мережевої прикладної програми списку бажаних засобів безпеки обладнання користувача, які будуть використовуватися, засоби безпеки списку замовляються перевагою

функції мережевої прикладної програми. У Блоці 6В список відсилається до бази даних параметрів безпеки користувача через функцію сервера початкового завантаження. У Блоці 6С функція мережевої прикладної програми одержує через функцію сервера початкового завантаження відклик засобу безпеки, що включає ключ безпеки, отриманий з інформації, що зберігається в базі даних, відповідаючи бажаному засобу безпеки, що міститься у списку, у
 5 такий спосіб повідомляючи функції мережевої прикладної програми щодо доступності принаймні одного з бажаних засобів безпеки в обладнанні користувача.

[0047] Метод як у попередньому параграфі, де відклик засобу безпеки включає індикацію засобів безпеки, розповсюджених до списку, та де засоби загальної безпеки замовляються як
 10 отримані з інформації, що зберігається в базі даних

[0048] Метод як у попередніх параграфах, де ключ відповідає, при наявності, самому привілейованому засобу безпеки, інакше ключ, відповідає менш привілейованому засобу безпеки.

[0049] Метод як у попередніх параграфах, де список відсилається до бази даних параметрів безпеки користувача через сервер абонентських даних.
 15

[0050] Метод як показано на Рисунку 6, де база даних є зовнішньою до системи, яка містить мережеву прикладну функцію та функцію сервера початкового завантаження.

[0051] Метод як у попередніх параграфах, де база даних включає поле для зберігання підтримуваних засобів безпеки.

[0052] Метод як у попередніх параграфах, де список містить одиничну точку входу, або містить дві або більше точок входу.
 20

[0053] Метод як у попередніх параграфах, де список відсилається у повідомлення запиту засобів безпеки.

[0054] Метод як у попередньому параграфі, повідомлення запиту засобів безпеки посилається, використовуючи пару атрибут-значення повідомлення протоколу Diameter.
 25

[0055] Різні блоки, показані на Фігурі 6, можуть бути розглянуті як етапи методу, та/або як операції, які впливають із дії коду комп'ютерної програми, та/або як множина подвійних логічних елементів кругообігу, побудованих, щоб виконати зв'язану функцію(ї).

[0056] Типові втілення також охоплюють обладнання, що включає процесор та запам'ятовуючий пристрій, включаючи код комп'ютерної програми, де запам'ятовуючий пристрій та код комп'ютерної програми, зконфігуровані із процесором, змушують обладнання принаймні виконувати визначення у функції мережевої прикладної програми списку бажаних засобів безпеки обладнання користувача, які будуть використовуватися, засоби безпеки списку замовляються перевагою функції мережевої прикладної програми, відсилати список у базу даних параметрів безпеки користувача через функцію сервера початкового завантаження, та одержувати через функцію сервера початкового завантаження відклик засобу безпеки, що включає ключ безпеки, отриманий з інформації, що зберігається в базі даних, ключ відповідає бажаному засобу безпеки, що міститься в списку, у такий спосіб повідомляючи функції мережевої прикладної програми щодо доступності принаймні одного з бажаних засобів безпеки в обладнанні користувача.
 30
 35
 40

[0057] Загалом, різні типові втілення можуть бути здійснені в апаратних засобах або схемах спеціального призначення, програмному забезпеченні, логічній схемі або будь-якій їх комбінації. Наприклад, деякі аспекти можуть бути виконані в апаратних засобах, у той час як інші аспекти можуть бути виконані в програмно-апаратних засобах або програмному забезпеченні, які можуть бути виконані контролером, мікропроцесором або іншим обчислювальним пристроєм, хоча винахід це не обмежує. У той час як різні аспекти типових втілень даного винаходу можуть бути проілюстровані та описані як блок-схеми, схеми послідовності операцій, або із використанням деякого іншого графічного представлення, добре зрозуміло, що ці блоки, обладнання, системи, засоби або методи, описані тут, можуть бути виконані, як необмежуючі приклади, у апаратних засобах, програмному забезпеченні, програмно-апаратних засобах, схемах спеціального призначення або логічних схемах, апаратних засобах або контролері загального призначення або інших обчислювальних пристроїв, або деякої їх комбінації.
 45
 50

[0058] У такий спосіб повинно бути зрозуміло, що принаймні деякі аспекти типових втілень винаходів можуть практикуватися в різних компонентах, таких як чипи та модулі інтегральної схеми, та що типові втілення даного винаходу можуть бути реалізовані в обладнанні, що втілюється як інтегральна схема. Інтегральна схема, або схеми, може включати компоновку схем (так само як можливо програмно-апаратні засоби) для того, щоб втілити принаймні один або більше процесор даних або процесорів даних, процесор цифрового сигналу або процесори, схему немодульованої передачі та радіочастотну схему, які зконфігуровані, щоб функціонувати відповідно до типових втілень даного винаходу.
 55
 60

[0059] Різні модифікації та адаптації вищезгаданих типових втілень даного винаходу можуть стати очевидними для тих, хто кваліфікований у відповідних галузях через вищезгаданий опис, коли читати в поєднанні із супровідними рисунками. Однак, будь-яка та всі модифікації будуть усе ще перебувати в межах обсягу необмежуючих та типових втілень даного винаходу.

5 [0060] Наприклад, у той час як типові втілення були описані вище в контексті архітектури GBA, потрібно розуміти, що типові втілення даного винаходу не обмежені для використання тільки з цим особливим типом системи, та що вони можуть використовуватися, щоб надавати переваги в інших системах.

10 [0061] Потрібно відзначити, що терміни "зв'язані", "з'єднані", або будь-який їх різновид, означає будь-який зв'язок або з'єднання, або пряме або непряме, між двома або більше елементами, та може охопити наявність одного або більше проміжних елементів між двома елементами, які "зв'язуються" або "з'єднуються" разом. З'єднання або зв'язок між елементами можуть бути фізичним, логічним, або їх комбінацією. Як використовується тут, два елементи можуть розглядатися як "зв'язані" або "з'єднані" разом за допомогою одного або більш проводів,

15 кабелів та/або друкованих електричних з'єднань, так само як за допомогою електромагнітної енергії, такої як електромагнітна енергія, що має довжину хвилі в радіочастотному діапазоні, мікрохвильовому діапазоні та оптичному (як видимому, так і невидимому) діапазоні, як декілька необмежуючих та невичерпних прикладів.

20 [0062] Додатково, різні імена, використані для описаних функцій (наприклад, NAF, HSS, BSF, та т.д.), інтерфейсів протоколу (наприклад, Zn, Zn', Zh, Zpn, Zpn', та т.д.), засобів сервісу (наприклад, GPL U, GBA U, та т.д.) та елементів (наприклад, ussType complexType) не призначені, щоб бути обмеженими у будь-якому відношенні, оскільки ці різні функції, інтерфейси, засоби сервісу, елементи та т.п. можуть бути ідентифіковані будь-якими відповідними іменами.

25 [0063] Крім того, деякі з засобів різних необмежуючих та типових втілень даного винаходу можуть бути використані, щоб надавати перевагу без відповідного використання інших засобів. По суті, вищезгаданий опис потрібно розглядати лише як ілюстрацію принципів, ідей та типових втілень даного винаходу, та не обмежувати його.

30 ФОРМУЛА ВІНАХОДУ

1. Спосіб бездротового зв'язку, що включає:

визначення у функції мережевої прикладної програми списку бажаних засобів безпеки обладнання користувача, які будуть використовуватися, засоби безпеки списку замовляються перевагою функції мережевої прикладної програми;

35 відсилання списку до бази даних параметрів безпеки користувача через функцію сервера початкового завантаження; та

одержання функцією мережевої прикладної програми, через функцію сервера початкового завантаження, відклику засобів безпеки, що включає ключ безпеки, отриманий з інформації, що зберігається в базі даних, відповідаючи бажаному засобу безпеки, що міститься в списку, у

40 такий спосіб повідомляючи функції мережевої прикладної програми щодо доступності принаймні одного з бажаних засобів безпеки в обладнанні користувача.

2. Спосіб за п. 1, де список відсилають до бази даних параметрів безпеки користувача через сервер абонентських даних.

3. Спосіб за п. 1, де база даних є зовнішньою до системи, що містить мережеву прикладну функцію та функцію сервера початкового завантаження.

4. Спосіб за п. 1, де база даних включає поле для зберігання підтримуваних засобів безпеки.

5. Спосіб за п. 1, де список містить одиничну точку входу або містить дві або більше точок входу.

50 6. Спосіб за п. 1, де список відсилають у повідомлення запиту засобів безпеки.

7. Спосіб за п. 6, де повідомлення запиту засобів безпеки посилають із використанням пари атрибут-значення повідомлення протоколу Diameter.

8. Спосіб за п. 6, де повідомлення запиту засобів безпеки включає бажані засоби безпеки обладнання користувача, відділені крапками з комою в їхньому привілейованому замовленні.

55 9. Постійно запам'ятовуючий комп'ютерозчитувальний носій, що включає команди комп'ютерної програми, які виконуються принаймні одним процесором для здійснення наступних операцій: визначення у функції мережевої прикладної програми списку бажаних засобів безпеки обладнання користувача, які будуть використовуватися, причому засоби безпеки списку замовляються перевагою функції мережевої прикладної програми;

відсилання списку до бази даних параметрів безпеки користувача через функцію сервера початкового завантаження; та

одержання функцією мережевої прикладної програми, через функцію сервера початкового завантаження, відклику засобів безпеки, що включає ключ безпеки, отриманий з інформації, що зберігається в базі даних, відповідаючи бажаному засобу безпеки, що міститься в списку, у

5

такий спосіб повідомляючи функції мережевої прикладної програми щодо доступності принаймні одного з бажаних засобів безпеки в обладнанні користувача.

10. Носій за п. 9, в якому відклик засобів безпеки включає індикацію засобів безпеки, розповсюджених до списку, та де засоби загальної безпеки замовлені як отримані з інформації, що зберігається в базі даних.

10

11. Носій за п. 9, де список надіслано до бази даних параметрів безпеки користувача через сервер абонентських даних.

12. Носій за п. 9, де база даних є зовнішньою до системи, що містить мережеву прикладну функцію та функцію сервера початкового завантаження.

15

13. Пристрій для бездротового зв'язку, що включає:

принаймні один процесор; та

принаймні один запам'ятовуючий пристрій, що включає комп'ютерний програмний код, де принаймні один запам'ятовуючий пристрій та комп'ютерний програмний код сконфігуровані принаймні з одним процесором, для здійснення принаймні наступних дій:

20

визначати у функції мережевої прикладної програми список бажаних засобів безпеки обладнання користувача, які будуть використовуватися, засоби безпеки списку замовляються перевагою функції мережевої прикладної програми;

відсилати список до бази даних параметрів безпеки користувача через функцію сервера початкового завантаження; та

25

одержувати функцією мережевої прикладної програми, через функцію сервера початкового завантаження, відклику засобів безпеки, що включає ключ безпеки, отриманий з інформації, що зберігається в базі даних, відповідаючи бажаному засобу безпеки, що міститься в списку, у такий спосіб повідомляючи функції мережевої прикладної програми щодо доступності принаймні одного з бажаних засобів безпеки в обладнанні користувача.

30

14. Пристрій за п. 13, де список надіслано до бази даних параметрів безпеки користувача через сервер абонентських даних.

15. Пристрій за п. 13, де база даних є зовнішньою до системи, що містить мережеву прикладну функцію та функцію сервера початкового завантаження.

16. Пристрій за п. 13, де база даних включає поле для зберігання підтримуваних засобів безпеки.

35

17. Пристрій за п. 13, де список містить одиничну точку входу або містить дві або більше точок входу.

18. Пристрій за п. 13, де список надіслано у повідомлення запиту засобів безпеки.

19. Пристрій за п. 18, де повідомлення запиту засобів безпеки надіслано із використанням пари атрибут-значення повідомлення протоколу Diameter.

40

20. Пристрій за п. 18, де повідомлення запиту засобів безпеки включає бажані засоби безпеки обладнання користувача, відділені крапками з комою в їхньому привілейованому замовленні.

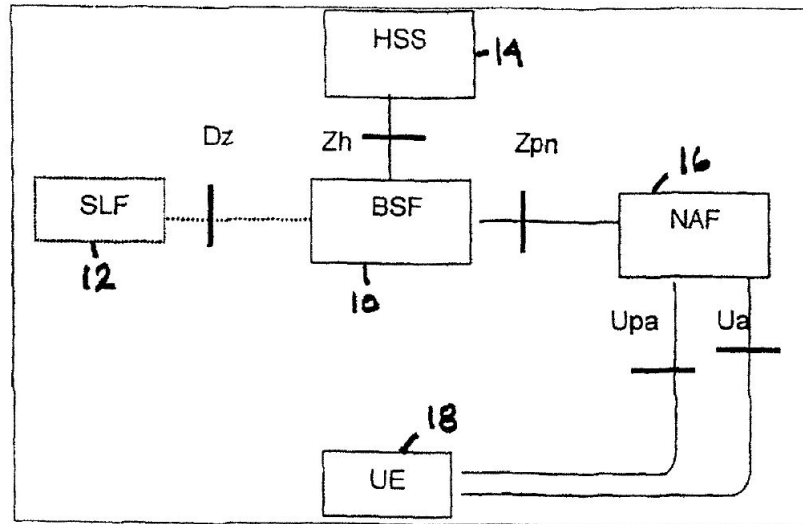


Fig. 1

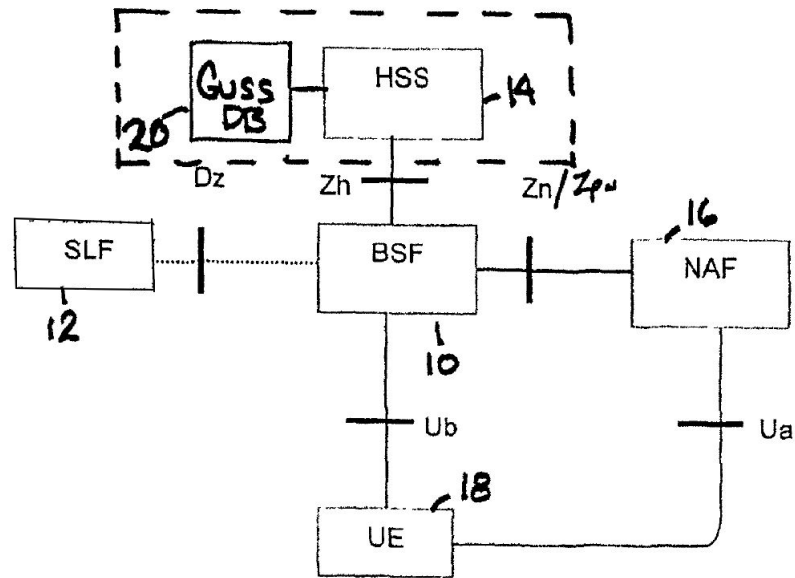


Fig. 2

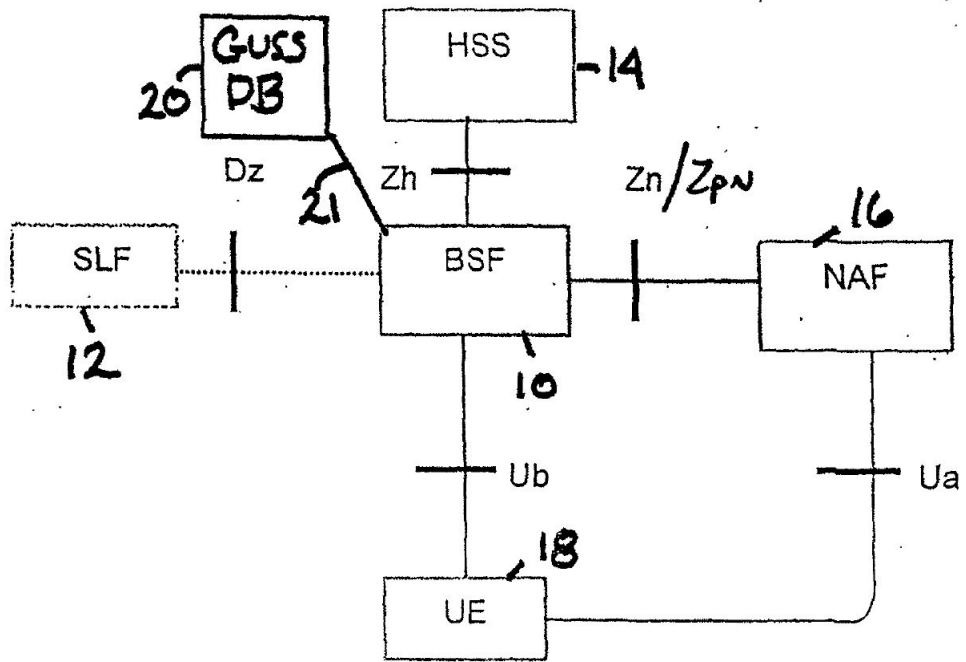


Fig. 3

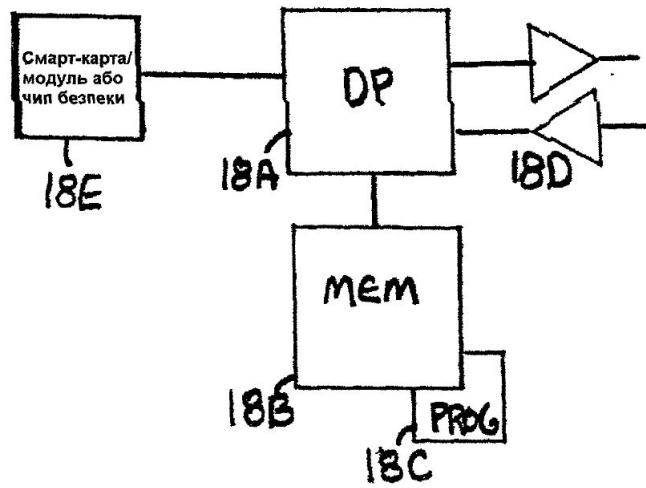
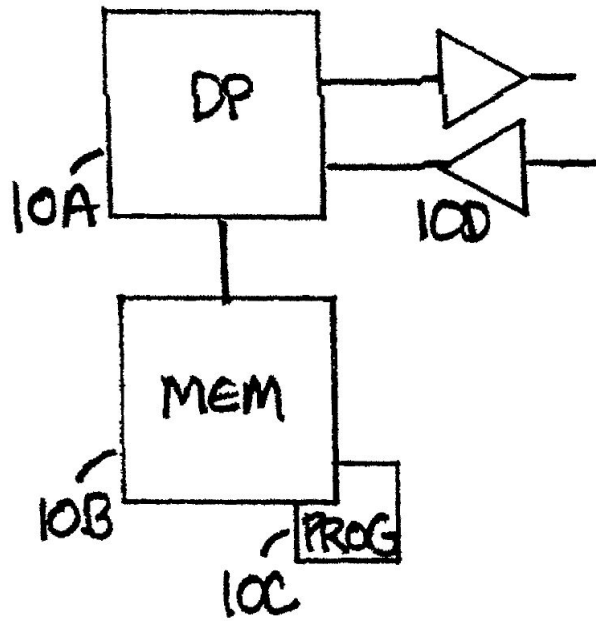
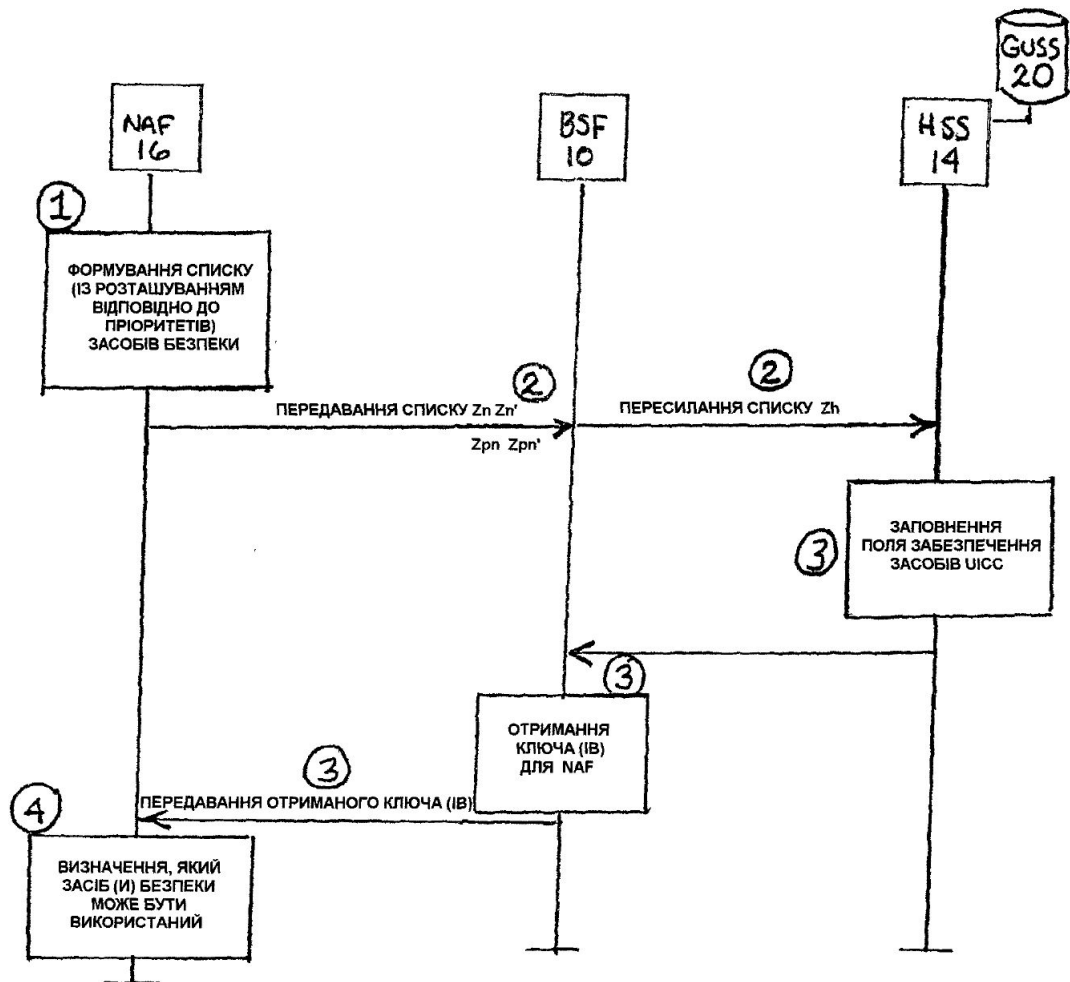


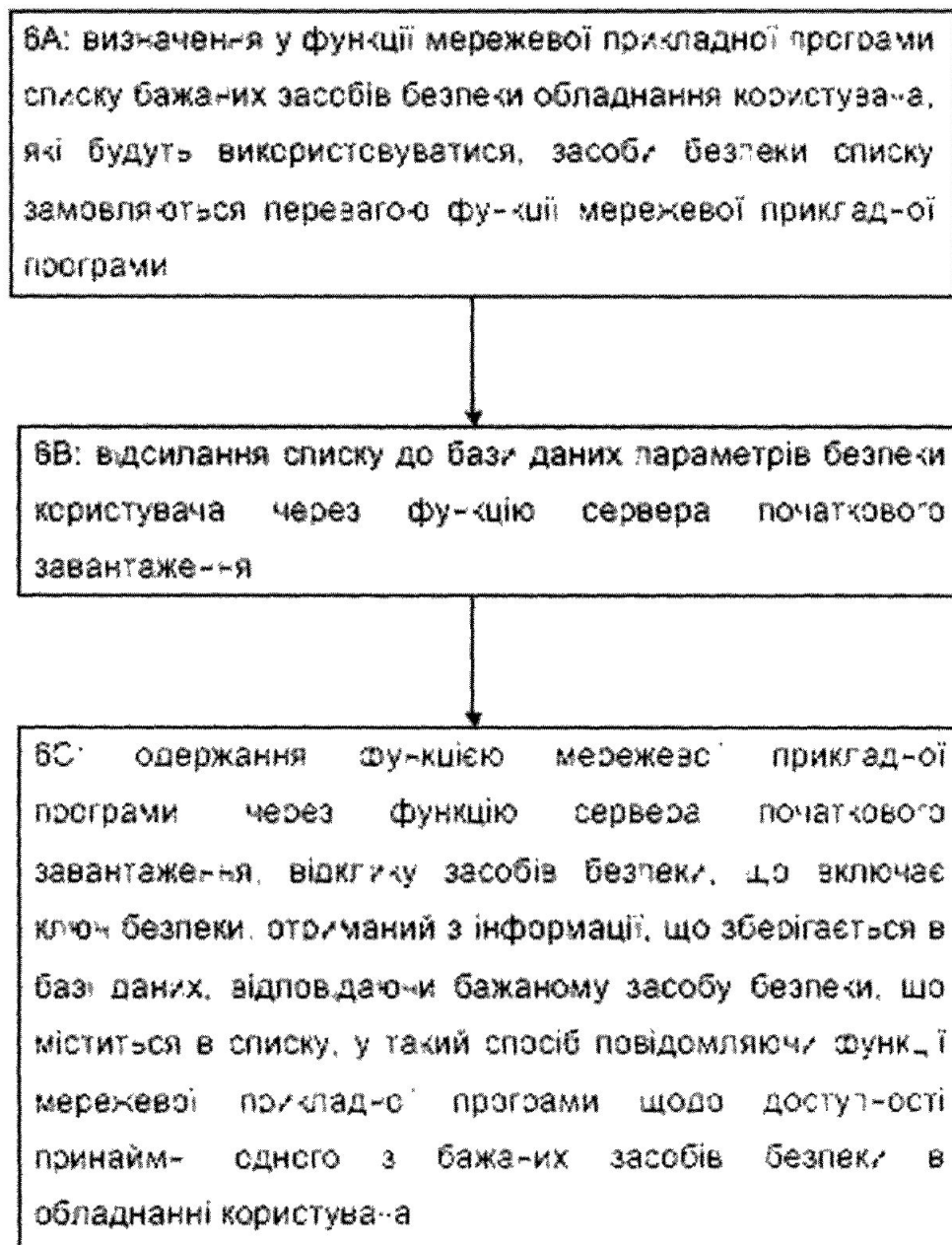
Fig. 4A



Фіг.4В



Фіг.5



Фіг.6