RZECZPOSPOLITA POLSKA

(12) **TŁUMACZENIE PATENTU EUROPEJSKIEGO**

(19) **PL**

(11) **PL/EP 2997550**

(13) **T3**

(51) Int.Cl.
G07C 9/00 (2006.01)
B60R 25/24 (2013.01)

(96) Data i numer zgłoszenia patentu europejskiego:
13.01.2015 15700657.8

(97) O udzieleniu patentu europejskiego ogłoszono:
08.06.2016 Europejski Biuletyn Patentowy 2016/23
EP 2997550 B1

Urząd Patentowy Rzeczypospolitej Polskiej

(54) Tytuł wynalazku:

SPOSÓB KONTROLI DOSTĘPU

(30) Pierwszeństwo:
22.05.2014 DE 102014107242

(43) Zgłoszenie ogłoszono:
23.03.2016 w Europejskim Biuletynie Patentowym nr 2016/12

(45) O złożeniu tłumaczenia patentu ogłoszono:
30.12.2016 Wiadomości Urzędu Patentowego 2016/12

(73) Uprawniony z patentu:
Huf Hülsbeck & Fürst GmbH & Co. KG, Velbert, DE

(72) Twórca(y) wynalazku:
SVEN GENNERMANN, Velbert, DE
DANIEL BAMBECK, Essen, DE

(74) Pełnomocnik:
rzecz. pat. Marta Skrobot
SULIMA GRABOWSKA SIERZPUTOWSKA
BIURO PATENTÓW I ZNAKÓW TOWAROWYCH SP.J.
Skr. poczt. 6
00-956 Warszawa 10

PL/EP 2997550 T3

Opis

[0001] Wynalazek dotyczy sposobu kontroli dostępu jednostek do zespołów fizycznych. Wynalazek dotyczy w szczególności systemu oraz sposobu, według którego można przydzielać jednostkom indywidualne uprawnienia dostępu oraz zarządzać nimi.

[0002] Zarządzanie prawami dostępu lub prawami korzystania można znaleźć w wielu miejscach w dziedzinie techniki. Istnieją na przykład złożone hierarchie praw oraz schematy praw w zarządzaniu uprawnieniami dostępu w systemach komputerowych. Jednostce, która sama legitymuje się przed systemem komputerowym na przykład za pomocą tajnego identyfikatora lub danych biometrycznych, przyznaje się tam dostęp do usług lub danych systemu obliczeniowego. Jeśli jednak przydzielone prawa lub uprawnienia nie wystarczają, aby przeprowadzić żądaną akcję, jest ona wstrzymywana za pomocą środków technicznych.

[0003] Ponadto znane są systemy blokujące, w których w celu kontroli dostępu identyfikowany jest środek blokujący, aby sprawdzić dostęp do danej funkcji, na przykład dostęp do danego obszaru. W tego rodzaju systemach często wychodzi się od tego, że posiadacz środka blokującego jest również uprawionym do żądania danej funkcji. Odpowiednie idee można znaleźć również w dziedzinie systemów blokady pojazdów, w szczególności w systemach typu „keyless-entry" oraz „keyless-go". Tam użytkownik nosi ze sobą kluczyki samochodowe, określane jako nośnik danych identyfikacyjnych. Ten nośnik danych identyfikacyjnych zawiera zakodowane informacje, które uznają uprawnienia nośnika danych identyfikacyjnych (niekoniecznie posiadacza nośnika danych identyfikacyjnych) do wykonywania funkcji w odniesieniu do samochodu. Jeśli zatem nośnik danych identyfikacyjnych zostanie przekazany kolejnemu użytkownikowi, to ten będzie również w stanie uruchomić i obsługiwać funkcje pojazdu za pomocą tego nośnika danych identyfikacyjnych.

[0004] W dziedzinie systemów dostępu dla pojazdów znanych jest wiele różnych systemów zarządzania, mających na celu zezwalanie na dostęp do pojazdów. Na przykład US 2013/0259232 A1 opisuje system sprzężenia lub kojarzenia (pairing) telefonu komórkowego z pojazdem w celu umożliwienia sterowania funkcjami pojazdu za pomocą telefon komórkowego.

[0005] DE 10 2011 078 018 A1 opisuje inny system do uruchamiania funkcji pojazdu, przy czym część komunikacji z pojazdem przeprowadza centrala telematyczna.

[0006] US2012/0164989 dotyczy innego sposobu oraz systemu bezprzewodowej funkcji zamykania pojazdu.

[0007] EP 1 910 134 B1 (WO2007/009453 A2) opisuje system o zarządzaniu centralnym, który rozdziela pakiety danych jako klucze na przenośnych urządzeniach dostępu.

[0008] Znane systemy i sposoby, które umożliwiają dostęp do urządzeń technicznych, mają jednak wady. W przypadku niektórych z tych systemów, za pomocą urządzeń technicznych, takich jak komputery przenośne, smartfony lub tym podobne, uprawnienie dostępu do urządzeń technicznych lub do uruchamiania funkcji można wygenerować lub wywołać w taki sposób, że do urządzeń (np. pojazdów) lub ich funkcji nieuprawniony dostęp może uzyskać intruz.

[0009] Zadaniem wynalazku jest dostarczenie pewnego i elastycznego sposobu umożliwienia poszerzonego zarządzania uprawnieniami dostępu do zespołów fizycznych.

[0010] Zgodnie z wynalazkiem zaproponowano sposób według zastrzeżeń 1-14.

[0011] Zgodnie z wynalazkiem, odnośnie tworzenia relacji komunikacyjnych oraz przenoszenia danych zbudowano relację czworoboczną, w której z jednej strony platforma kontrolująca może wchodzić w połączenie komunikujące zarówno z przenośnym urządzeniem dostępu, jak i jednostką kontroli dostępu kontrolowanego zespołu fizycznego. Użytkownik współdziała ze swojej strony z przenośnym urządzeniem dostępu. Ewentualnie

współdziała on także z platformą centralną przy użyciu osobnych ścieżek komunikacji (np. komputer z dostępem do Internetu). Tożsamość użytkownika jest składnikiem kluczowym, który umożliwia współdziałanie innych składników, przy czym tożsamość jest sprawdzana w różnych etapach. Ta komunikacja między różnymi składnikami nie musi koniecznie przebiegać jednocześnie, jest jednak istotne, aby zasadnicze możliwości komunikacyjne tych trzech składników były wymienne między sobą. Ta idea zapewnia weryfikację informacji, otrzymanych z jednej z transmisji z niezależnym miejscem. Jak opisano poniżej, ta relacja przemienna w połączeniu ze specyfiką przenośnego urządzenia dostępu zapewnia dostęp w szczególnie pewny i niezawodny sposób.

[0012] Użytkownik zgodnego z wynalazkiem sposobu ma dostęp do przenośnego urządzenia dostępu, zatem na przykład do smartfona z zainstalowaną na nim aplikacją. Nawet gdyby mógł doprowadzić do komunikacji tego urządzenia z jednostką kontroli dostępu po stronie pojazdu, jednostka kontroli dostępu po stronie pojazdu bez problemu nie zezwoliłby na dostęp do pojazdu, ponieważ brakowałoby wymaganego uprawnienia. Jako uprawnienie pojazd akceptuje mianowicie nie samą tożsamość przenośnego urządzenia dostępu, ale tylko w połączeniue ze zweryfikowaną tożsamością użytkownika. To wykrywanie tożsamości udaje się tylko poprzez to, że przenośne urządzenie dostępu otrzymuje informacje z platformy centralnej, które charakteryzują przenośne urządzenie dostępu oraz osobę, zidentyfikowaną za jego pomocą jako uprawniony użytkownik zespołu fizycznego.

[0013] Wynalazek wyodrębnia zarządzanie uprawnieniami oraz kontrolowanym zespołem fizycznym w centralnej platformie sterującej. Tym samym to zarządzanie jest chronione przed manipulacją przez nieuprawnione osoby, ponieważ tylko godne zaufania stanowiska mogą przeprowadzać zmiany na centralnej platformie sterującej. Nie wystarczy manipulacja danymi z urządzenia przenośnego, ponieważ jednostka kontroli dostępu po połączeniu z platformą centralną weryfikuje dane uprawnień.

[0014] Centralna platforma sterująca może zawierać informacje na temat jednostek ludzkich, które są identyfikowane przed tą platformą sterującą w niezawodny sposób. Centralna platforma sterująca może jednak również zarządzać przypisanymi do anonimowych identyfikatorów prawami do przypisanej jednostki kontroli dostępu, tak że w centralnej platformie sterującej nie istnieją żadne skojarzenia z prawdziwymi osobami, lecz tylko anonimowe identyfikatory.

[0015] Podczas gdy w tradycyjnych systemach dostępu lub zarządzaniu dostępem identyfikacja następuje za pomocą odpowiedniego narzędzia, znacznika, klucza, karty kodowej lub tym podobnych, zgodnie z wynalazkiem uprawnienia są zarządzane i przyznawane osobom lub niepowtarzalnym identyfikatorom. Niezależnie od tego, którym środkiem posługuje się osoba w celu wylegitymowania się przed centralną platformą sterującą lub urządzeniem dostępu, przydzielenie uprawnień nie jest związane z takim środkiem (telefon, klucz, etc.), lecz z rozpoznaną osobą względnie rozpoznaną tożsamością.

[0016] Istotne dla wynalazku jest to, że w centralnej platformie sterującej zapisywane są prawa przypisywane do tożsamości osoby lub anonimowych identyfikatorów. Te prawa dotyczą każdorazowo częściowych zbiorów jednostek kontroli dostępu, które są zarządzane przez platformę centralną. Do identyfikatora mogą zatem na przykład zostać przyznane prawa, które obowiązują dla grup lub także wszystkich przyporządkowanych jednostek kontroli dostępu. Inne prawa mogą być przyporządkowane dla pojedynczych jednostek kontroli dostępu. Na przykładzie kontroli taboru oznacza to, że członkowi personelu zarządzającego np. prawo do otwierania pojazdu przydziela się odnośnie wszystkich pojazdów taboru, jednak prawo do uruchomienia pojazdu jedynie odnośnie kilku pojazdów.

[0017] Podobnie jest konieczne, aby najpierw wprowadzić do centralnej platformy sterującej wpis dotyczący tożsamości lub anonimowego identyfikatora dopuszczonego użytkownika. Te wpisy mogą być zarządzane w tradycyjny sposób za pomocą bazy danych, która udostępnia interfejs do zapytań. Dzięki interfejsom do innych systemów, np. systemów

oferentów samochodów do wynajęcia, agencji ochrony lub oferentów „car-sharing”, może nastąpić również przejęcie identyfikatora. Podczas gdy sprzężone systemy kolejnych oferentów znają tożsamość swoich klientów, przekazują one platformie centralnej np. tylko anonimowy identyfikator oraz przynależne prawa. Dane osobowe pozostają wówczas u kontrahenta, platforma centralna jednak zarządza prawami za pomocą identyfikatora.

[0018] Przenośne urządzenie dostępu może wystąpić komunikacja danych z centralną platformą sterującą. Z centralnej platformy sterującej przenośnemu urządzeniu dostępu udostępniane są informacje, które umożliwiają legitymowanie się przed jednostką kontroli dostępu zespołu fizycznego. Może to być np. certyfikat, który jest wystawiany przez centralną platformę sterującą.

[0019] Przenośne urządzenie dostępu służy poza tym do tego, aby zabezpieczyć przed jednostką kontroli dostępu tożsamość posiadacza. Przenośne urządzenie dostępu jest w tym celu tak wyposażone, że możliwa jest niezawodna identyfikacja użytkownika. Ta identyfikacja użytkownika może na przykład nastąpić dzięki znanemu tylko jemu identyfikatorowi lub dzięki zapytaniu o dane biometryczne, jak na przykład rozpoznawanie twarzy, analiza głosu lub odcisku palca. Dopiero gdy ta identyfikacja przed przenośnym urządzeniem dostępu jest skuteczna, można uzyskać dostęp do informacji w przenośnym urządzeniu dostępu. Rodzaj koniecznej identyfikacji może zależeć od ważności żądanego prawa pod względem bezpieczeństwa. Jeśli użytkownik żąda np. zapytania o dane pojazdu (stan licznika kilometrów, zawartość zbiornika) bezpośrednio w pobliżu pojazdu, może wystarczyć podanie numeru PIN na urządzeniu przenośnym lub szczególny ruch wycierający na panelu sterowania urządzenia. Do uruchomienia pojazdu jest konieczne np. rozpoznawanie twarzy. To, który rodzaj sprawdzania tożsamości jest konieczny dla którego uprawnienia, może zostać zdeponowane na platformie centralnej.

[0020] Jeśli identyfikacja przed przenośnym urządzeniem dostępu jest skuteczna, zostaje utworzone połączenie z kontrolowanym zespołem fizycznym, dokładniej z jednostką kontroli dostępu zespołu fizycznego, a informacje dostępu, które co najmniej częściowo zostały przekazane przez centralną platformę sterującą do przenośnego urządzenia dostępu, są wykorzystywane, aby mieć dostęp do funkcji zespołu fizycznego.

[0021] Przy tym zgodne z wynalazkiem połączenie jednostki kontroli dostępu z centralną platformą sterującą dochodzi do skutku po stronie zespołu fizycznego. Dzięki temu połączeniu jest możliwe, aby jednostka kontroli dostępu po stronie zespołu fizycznego weryfikowała, czy informacje o dostępie, przekazane przez przenośne urządzenie dostępu, są rzeczywiście uprawnionymi danymi dotyczącymi dostępu do żądanych funkcji. Tradycyjne systemy nie dysponują takim połączeniem i muszą w związku z tym polegać na sprawdzaniu danych jedynie z przenośnego urządzenia dostępu.

[0022] Centralna platforma sterująca zna zarówno zespoły uczestniczące w procesie legitymowania, jak również uprawnienia osoby zidentyfikowanej, przypisane za pomocą tych zespołów. Centralnej platformie sterującej jest znana z jednej strony tożsamość lub identyfikator użytkownika, z drugiej strony tożsamość przenośnego urządzenia dostępu i tożsamość jednostki kontroli dostępu w zespole fizycznym. Wszystkie te urządzenia są identyfikowane za pomocą niepowtarzalnych cech. Tylko centralna platforma sterująca dysponuje całą wiedzą w celu umożliwienia dostępu do zarządzania centralnego.

[0023] W prostej postaci wynalazku na platformie centralnej jest umieszczony identyfikator, który charakteryzuje użytkownika. W identyfikatorze są wpisywane i kojarzone dane z przenośnego urządzenia dostępu. Na przykład może on zawierać numer IMEI dla urządzenia przenośnego. Poza tym w platformie centralnej zapisywany jest rekord praw dostępu do identyfikatora. Ta pierwsza identyfikacja następuje np. za pośrednictwem miejsca zaufanego, np. urzędu lub zaufanego usługodawcy.

[0024] Przed pierwszym użyciem przez platformę centralną wysyłana jest wiadomość do zarejestrowanego urządzenia przenośnego, które ma służyć jako przenośne urządzenie dostępu. Od użytkownika urządzenia żąda się poddania się pierwszej rejestracji. Użytkownik

podaje wówczas na urządzeniu przenośnym szereg informacji, które później są wykorzystywane do sprawdzania tożsamości. Zapisywany jest na przykład numer PIN, ruch wycierający i pobierane są dane biometryczne do porównania (skan twarzy, próbka głosu, odcisk palca, itp.). Gdy to nastąpi, dane mogą już być wywołane przez platformę centralną i zapisane na przenośnym urządzeniu dostępu. Te dane mogą zawierać np. dane identyfikacyjne, jak również dane, które potwierdzają autentyczność danych. Dane mogą być na przykład oznakowane certyfikatem platformy centralnej lub także być zakodowane. Następnie system jest gotowy do użytku.

[0025] Jeśli użytkownik chce mieć dostęp do urządzenia fizycznego, np. pojazdu, musi się znaleźć w pobliżu zespołu fizycznego z przyporządkowaną jednostką kontroli dostępu. Najpierw musi on wylegitymować się przed przenośnym urządzeniem dostępu. Dopiero gdy to się powiedzie, przenośne urządzenie dostępu ma na ogół dostęp do danych, zapisanych na przenośnym urządzeniu dostępu, i przekazuje te dane do żądanego prawa do jednostki kontroli dostępu, która zarządza prawami do zespołu fizycznego. To przekazanie następuje przez połączenie bezprzewodowe, np. przez Bluetooth, WLAN, lub NFC. Po stronie jednostki kontroli dostępu sprawdza się, czy dane są autentyczne. Poniżej zostanie to wyjaśnione dokładniej. Jednostka kontroli dostępu ma przy tym dostęp do danych, które otrzymał on bezpośrednio przez połączenie komunikujące od platformy centralnej (bezpośrednio w trakcie aktualnego sprawdzania praw lub przesunięte w czasie, już do wcześniejszego momentu).

[0026] Dzięki objaśnionej wcześniej wzajemnej komunikacji składników można ustanowić nadzwyczaj pewne ograniczenia dostępu. Tradycyjne systemy były zdane na to, by przeprowadzić sprawdzenie autentyczności na podstawie danych zapisanych trwale w jednostce kontroli dostępu. Tam były trwale zdeponowane np. certyfikaty zaufanych stanowisk. Zgodna z wynalazkiem możliwość aktualizacji danych, aż do sprawdzania w czasie rzeczywistym, zabezpiecza dostęp, ponieważ ta ścieżka komunikacji jest niezależna od ścieżki pomiędzy przenośnym urządzeniem dostępu a platformą centralną, a także niezależna od danych na przenośnym urządzeniu dostępu, które zostały ewentualnie zmanipulowane.

[0027] Korzystnie przenośnemu urządzeniu dostępu przekazywany jest klucz lub certyfikat dostępu do określonej, przyporządkowanej jednostce kontroli dostępu zespołu fizycznego. Przyporządkowanej jednostce kontroli dostępu zespołu fizycznego platforma centralna przekazuje np. część asymetrycznego klucza w celu zweryfikowania certyfikatu. Przy tym można zastosować tradycyjne asymetryczne sposoby kodowania, na przykład zgodnie z ideą klucza publicznego i prywatnego.

[0028] Zaleta tego rodzaju kontroli dostępu polega na tym, że wprawdzie w szczególności w celu instalacji i ustanowienia praw dostępu musi dojść do połączenia wszystkich uczestników komunikacji z centralną platformą sterującą, jednak w późniejszym czasie możliwa jest także przejściowa kontrola dostępu i funkcja dostępu bez udziału centralnej platformy sterującej. Na przykład centralna platforma sterująca może przekazać przenośnemu urządzeniu dostępu oraz jednostce kontroli dostępu w zespole fizycznym informacje, które są zaopatrzone w certyfikat centralnej platformy sterującej. Zarówno w przenośnym urządzeniu dostępu, jak i w zespole fizycznym oraz jednostce kontroli dostępu można przewidzieć, że w każdym przypadku czasowo zaufana będzie pewna klasa certyfikatu, na przykład takie certyfikaty, które są wystawione przez centralną platformę sterującą, również gdy chwilowo nie jest możliwy bezpośredni dostęp do centralnej platformy sterującej. W tym celu można zaopatrzyć certyfikaty w daty ważności, po upływie których certyfikaty nie będą już dłużej akceptowane do wzajemnego legitymowania.

[0029] Odnośnie identyfikacji użytkownika lub identyfikatora może tym samym istnieć wiele różnych schematów, dotyczących uprawnień dostępu do różnych zespołów fizycznych. Na przykład w przypadku zastosowania wynalazku do kontroli dostępu do pojazdów, dla jednej i tej samej tożsamości mogą zostać przyznane różne uprawnienia dla

różnych pojazdów, przy czym jednak elementem łączącym jest ta sama tożsamość osoby użytkownika. Na platformie sterującej w kontekście zarządzania uprawnieniami może również mieć miejsce rozszerzanie przyznawania praw lub ograniczanie praw, na przykład ograniczenie dotyczące rodzaju użytkowania lub zakresu użytkowania odnośnie określonego pojazdu (na przykład dozwolona prędkość maksymalna niezależnie od używanego pojazdu).

[0030] Wynalazek zostanie teraz objaśniony dokładniej za pomocą przykładów wykonania, które są pokazane na załączonych figurach.

Figura 1 ukazuje schemat przebiegu komunikacji według pierwszego przykładu wykonania wynalazku.

Figura 2 ukazuje schemat urządzenia oraz zarządzania platformą centralną według drugiego przykładu wykonania wynalazku.

Figura 3a ukazuje pierwszy schemat dostępu do pojazdu według drugiego przykładu wykonania wynalazku.

Figura 3b ukazuje drugi schemat dostępu do pojazdu według drugiego przykładu wykonania wynalazku.

[0031] Na figurze 1 przedstawiono symbolicznie różne stacje i oddzielne zespoły funkcyjne. Przebieg strumienia informacji i wymiany informacji w czasie jest przedstawiony strzałkami pomiędzy tymi zespołami. Kontrolowane zespoły fizyczne są w tym przypadku samochodami, w których jednostka kontroli dostępu jest sprzężona z centralnym systemem sterującym pojazdu, który kontroluje prawa do funkcji pojazdu i może dopuszczać i blokować funkcje.

[0032] Zanim sposób będzie mógł być realizowany w pokazany sposób, należy przeprowadzić proces uczenia. Oznacza to, że centralnej platformie sterującej są udostępniane informacje dotyczące tożsamości użytkowników oraz uprawnień, jak również kontrolowanych pojazdów. Może to na przykład stać się to, że dana osoba wylegitymuje się przed miejscem zaufanym odpowiednim środkiem identyfikacyjnym (np. paszportem lub dowodem osobistym). Tym miejscem zaufanym może być sprzedawca samochodów, który osobiście sprawdza tożsamość i kojarzy odpowiedni wpis dotyczący tożsamości z uprawnieniem dostępu do określonego pojazdu.

[0033] Te dane są wprowadzane przez sprzedawcę samochodów przy kupnie samochodu lub podczas prac konserwacyjnych do bazy danych, do której dostęp ma centralna platforma sterująca. Istotne jest to, że tożsamościami oraz przyporządkowanymi tożsamościom uprawnieniami zarządza się w centralnej platformie sterującej, a zmiany mogą być przeprowadzane jedynie za pośrednictwem centralnej platformy sterującej. Korzystanie z systemu centralnego może odbywać się w tradycyjny sposób, np. poprzez zarządzanie bazą danych za pomocą maski wprowadzania, która jest przedstawiona w przeglądarce internetowej. Właściwe zarządzanie pod front-endem może być dowolnym rodzajem bazy danych z odpowiednim zabezpieczeniem.

[0034] Zgodnie z wynalazkiem ma zatem miejsce zarządzanie uprawnieniami a więc w miejscu centralnym, mianowicie centralnej platformie sterującej. Poza tym centralna platforma sterująca informowana jest o zespołach fizycznych o kontrolowanym dostępie, w tym przypadku pojazdach. W tym celu w centralnej platformie sterującej zapisywana jest niepowtarzalna identyfikacja pojazdu. W przypadku zarządzania flotą lub w przypadku idei „car-sharing", wszystkie pojazdy mogą być zapisane w centralnej platformie sterującej jako zespoły fizyczne. Pojazdom przyporządkowywany jest każdorazowo jednoznacznie jednostka kontroli dostępu, która może połączyć się z centralną platformą sterującą.

[0035] Ostatecznie jest jeszcze istotne to, że centralna platforma sterująca informowana jest także o każdym przenośnym urządzeniu dostępu. Przenośne urządzenie dostępu może przy tym zostać przyporządkowane w centralnej platformie sterującej użytkownikowi lub identyfikatorowi, zatem zostać z nim skojarzone. Przebiega to na przykład tak, że identyfikowana osoba rejestruje przed miejscem zaufanym przenośne urządzenie dostępu, w tym przypadku smartfon. Na przykład podaje się numer telefonu. Na ten numer telefonu

przez miejsce zaufane może wówczas zostać wysłana wiadomość, przy czym treść wiadomości musi zostać wówczas z kolei podana przez identyfikowaną osobę miejscu zaufanemu. W ten sposób zamyka się cykl i weryfikuje się, czy rzeczywiście podana identyfikacja przenośnego urządzenia dostępu odpowiada identyfikowanej osobie.

[0036] Poniżej opisano zgodny z wynalazkiem sposób odnośnie jego zastosowania, przy czym powołano się na figurę 1.

[0037] Na początku procesu, poprzez wykonanie pewnej czynności użytkownika na smartfonie, użytkownik uzyskuje dostęp do pojazdu, w pobliżu którego znajduje się on wraz z urządzeniem przenośnym (np. smartfonem lub tabletem). Wprowadzenie dokonane przez użytkownika, na przykład wezwanie aplikacji na urządzeniu przenośnym, jest oznaczone strzałką komunikacyjną 1. Przenośne urządzenie dostępu weryfikuje tożsamość użytkownika, w tym przykładzie przeprowadzając rozpoznawanie twarzy (strzałka 2). Użytkownik pokazuje swoją twarz do kamery zintegrowanej w smartfonie, a oprogramowanie znajdujące się w urządzeniu porównuje twarz z zapisanymi i uwierzytelnionymi danymi biometrycznymi.

[0038] Jeśli to uwierzytelnianie przed urządzeniem przenośnym nie powiedzie się, proces zostaje przerwany w tym miejscu i próba dostępu do pojazdu nie udaje się.

[0039] Weryfikacja tożsamości może nastąpić na podstawie danych zapisanych w sposób zakodowany w urządzeniu przenośnym, zatem dane biometryczne mogą istnieć zapisane na urządzeniu przenośnym w sposób zakodowany.

[0040] Jeśli tożsamość jest skutecznie zweryfikowana przez urządzenie przenośne za pomocą wymiany komunikacyjnej 2, przenośne urządzenie dostępu nawiązuje kontakt z pojazdem, co może nastąpić poprzez standardowy interfejs NFC lub połączenie Bluetooth. Przenośna jednostka dostępu tworzy połączenie z jednostką kontroli dostępu pojazdu, co pokazano strzałką komunikacyjną 3. Przenośna jednostka dostępu żąda w tej wiadomości np. uruchomienia funkcji pojazdu, np. otworzenia drzwi.

[0041] Jednostka kontroli dostępu pojazdu jest wówczas informowana przez urządzenie przenośne o zweryfikowanej tożsamości użytkownika. Zgodnie z tym przykładem dzieje się tak za pomocą certyfikatów, które są wystawiane przez centralną platformę sterującą i są zapisywane w smartfonie. W szczególności mogą być do tego stosowane tradycyjne sposoby certyfikowania z kluczami publicznymi i prywatnymi. W urządzeniu przenośnym istnieje zatem na przykład informacja o tożsamości, która jest oznakowana kluczem prywatnym centralnej platformy sterującej. W jednostce kontroli dostępu w pojeździe, podobnie jak w przypadku przeglądarki internetowej, istnieją klucze certyfikatu głównego w postaci kluczy publicznych centralnej platformy sterującej. Jedynie, gdy przekazane informacje o tożsamości są informacjami prawidłowo certyfikowanymi, informacja o tożsamości może zostać odkodowana dla pojazdu i zostać rozpoznana jako prawidłowa.

[0042] Za pomocą tych informacji o tożsamości jednostki kontroli dostępu pojazdu zwraca się do platformy sterującej, co pokazano strzałką 4, i pyta o prawa dostępu, które istnieją dla tej tożsamości. Jednostka kontroli dostępu dysponuje w tym celu modułem GSM do komunikacji z platformą centralną za pomocą mobilnej sieci radiokomunikacyjnej. Strzałki 5 i 6 pokazują, że platforma sterująca ma dostęp zarówno do zarządzania tożsamościami, sprzężonego z platformą sterującą, jak również zarządzania uprawnieniami. Nie muszą one być umiejscowione w tym samym miejscu co centralna platforma sterująca. Na przykład w przypadku idei „car-sharing” może występować centralne zarządzanie tożsamościami, które, obejmując wiele firm, jest utrzymywane przez kilku oferentów „car-sharing”. Uprawnienia, które są przypisane tym tożsamościom, a zatem pytanie, czy dana osoba może uzyskać dostęp do określonego pojazdu w puli „car-sharing”, mogą być zapisane u każdej z firm. Jeśli zatem są różne firmy „car-sharing”, centralna platforma sterująca w zależności od wywoływanego zespołu samochodowego może mieć dostęp do centralnego zarządzania tożsamościami oraz do specjalnej puli uprawnień określonego oferenta „car-sharing”, do którego przynależy zidentyfikowany pojazd. W przypadku komunikacji pomiędzy pojazdem

a centralną platformą sterującą można również zastosować komunikację opartą na certyfikacie w celu zapewnienia autentyczności partnera komunikacji.

[0043] W centralnej platformie sterującej ustala się zatem, jakie uprawnienia ma zidentyfikowana osoba w odniesieniu do pojazdu. Uprawnienia mogą być na przykład tak ukształtowane, że dana osoba ma pełne prawa dostępu do pojazdu w zakresie otwierania drzwi oraz uruchamiania silnika. Alternatywnie może być tak, że zidentyfikowana osoba jest członkiem załogi warsztatu oferenta „car-sharing", który zasadniczo ma prawo otwierać wszystkie pojazdy, jednak nie ma prawa wykonywać przejazdów o prędkościach powyżej 20 km/h.

[0044] Ta informacja jest przekazywana z powrotem przez centralną platformę sterującą, strzałka 7, do zespołu sterowania dostępem w pojeździe, który to zespół wydaje odpowiednie ustawienia lub sygnały do systemu sterowania pojazdem. Zgodnie z tym system sterowania podejmuje odpowiednio na przykład odblokowanie drzwi, a uprawnienie do wykonywania kolejnych funkcji pojazdu zostaje włączone.

[0045] Podsumowując zapewnia się zatem to, że odbywa się sprawdzenie tożsamości, aby przenośne urządzenie dostępu mogło w ogóle zostać użyte. Po drugie przenośne urządzenie dostępu może być zaopatrzone w identyfikator certyfikowany przez centralną platformę sterującą, co zapewnia bezpieczeństwo w odniesieniu do wszystkich kontrolowanych za jej pomocą fizycznych zespołów.

[0046] Certyfikat w smartfonie w kolejnej postaci tego przykładu wykonania może mieć krótkoterminową czasową sekwencję, tak że przenośne urządzenie dostępu regularnie musi pobierać sobie odnowiony certyfikat z centralnej platformy sterującej przez łącze danych. Opisane w ten sposób rozwiązanie, oparte na certyfikacie i sprzężone ze sprawdzaniem tożsamości na urządzeniu przenośnym, ma więcej zalet. Zasadniczy, zgodny z wynalazkiem sposób wykorzystuje łącze danych pomiędzy pojazdem (jednostka kontroli dostępu) a centralną platformą sterującą w celu weryfikacji praw. To łącze nie jest jednak zawsze do dyspozycji, na przykład w przypadku przejazdów w terenie o gorszej jakości transmisji danych lub w przypadku garaży podziemnych. Jednakże sposób ten umożliwia w tym przypadku kontrolę dostępu za pomocą certyfikatów. Z jednej strony użytkownik musi się wylegitymować przed urządzeniem przenośnym, co jest możliwe na podstawie danych zapisanych w urządzeniu przenośnym. Jeśli ta weryfikacja się powiedzie, w urządzeniu przenośnym istnieją ważne, dotyczące certyfikatów dane z centralnej platformy sterującej, których ważność jeszcze nie wygasła. Tylko dzięki tym informacjom jest możliwe, aby po stronie pojazdu zostały zapewnione określone uprawnienia dotyczące dostępu do pojazdu, nawet jeśli nie podjęto bezpośredniej komunikacji z centralną platformą sterującą. Po stronie pojazdu, w jednostce kontroli dostępu, z wcześniejszych połączeń z platformą centralną istnieją zapisane informacje o certyfikatach z centralnej platformy sterującej i można to zweryfikować, że w przypadku zakończonej powodzeniem kontroli tożsamości obecny jest ważny certyfikat przenośnego urządzenia dostępu. Ten certyfikat może już na przykład wystarczyć, aby użytkownik mógł uzyskać dostęp do pojazdu i np. w przypadku prędkości maksymalnej, np. do 50 km/h mógł pokonać ograniczony odcinek drogi, np. maksymalnie 2 km, w czasie którego musi zostać nawiązana komunikacja pomiędzy jednostką kontroli dostępu a centralną platformą sterującą. Gdy tylko utworzone zostaje takie połączenie, następuje całkowite sprawdzenie oraz całkowite udzielenie uprawnień.

[0047] Ta idea tymczasowego zaufania na podstawie certyfikacji jest możliwa, ponieważ z jednej strony nastąpiła identyfikacja użytkownika przed urządzeniem przenośnym i o tej identyfikacji został poinformowany także pojazd, a z drugiej strony można potwierdzić przed pojazdem ustanowienie tymczasowego zaufania, opartego na certyfikacie. Taki sposób nie byłby możliwy, gdyby, tak jak w przypadku tradycyjnych sposobów, brakowało niepozostawiającego wątpliwości potwierdzania tożsamości. Ponieważ jednak ta tożsamość jest warunkiem, aby w ogóle w urządzeniu przenośnym uzyskać dostęp do istniejącego tam zakodowanego certyfikatu, pojazd może tolerować tymczasowe udzielenie zaufania oraz

przyznanie uprawnień. W ten sposób zgodny z wynalazkiem sposób jest lepszy od tradycyjnych sposobów, które każdorazowo wymagają wymuszonego połączenia z centralną platformą sterującą lub przenośnym urządzeniem dostępu, na przykład ufają kluczowi lub smartfonowi z odpowiednią aplikacją, bez konieczności weryfikacji tożsamości użytkownika.

[0048] W urządzeniu przenośnym można zapisać do tych celów liczne różne certyfikaty, na przykład dla różnych przedsiębiorstw „car-sharing". Poza tym udzielanie uprawnień może również odbywać sie na najróżniejsze sposoby. Na przykład w stosunku do danej tożsamości może zostać podjęte priorytetowe ustawienie uprawnień, które na przykład pozwala zasadniczo tylko na jazdę ze zredukowaną prędkością, niezależnie od właściwego zespołu samochodowego. Na przykład w przypadku kierowcy w określonym wieku, dla danej tożsamości można ustalić, że ten kierowca może jechać zasadniczo tylko z prędkością maksymalną wynoszącą np. 120 km/h. O tym uprawnieniu wyższej rangi, niezależnie od wywoływanego zespołu „car-sharing" lub zespołu floty, jest informowany pojazd, tak że na przykład jeden i ten sam pojazd jest napędzany w różnych trybach jazdy pojazdu w zależności od żądającej dostępu tożsamości. Ta postać jest możliwa tylko dzięki temu, że istnieje centralna platforma sterująca, która ma informacje o tożsamości, które z kolei mogą być sprzężone z różnymi ustawieniami uprawnień, także w przypadku różnych miejsc. Jedna i ta sama tożsamość może wylegitymować się za pomocą różnych urządzeń przenośnych przy różnych zespołach fizycznych. Jest to możliwe tylko dlatego, że tożsamość osoby jest weryfikowana w urządzeniu przenośnym, a przenośne urządzenie dostępu (smartfon) jako takie nie jest rozpoznawane jako uprawniony środek dostępu. W związku z tym sposób ten jest znacznie lepszy od takiego sposobu używania prostego kluczyka zapłonu, ponieważ tam nie zachodzi sprawdzanie tożsamości w połączeniu z urządzeniem przenośnym, a poza tym przenośne urządzenie dostępu w przypadku utraty lub kradzieży może zostać w łatwy sposób zablokowane zdalnie przed dostępem do pojazdu.

[0049] Wszystkie komunikacje, realizowane w zgodnym z wynalazkiem sposobie, mogą być przeprowadzone z tradycyjnymi zabezpieczeniami, np. przy utworzeniu połączeń według protokołu TLS w przypadku komunikacji, opartej na łączeniu z Internetem.

[0050] Po tym, jak w odniesieniu do figury 1 opisano zasadniczy i ogólny przebieg sposobu, poniżej opisany zostanie kolejny przykład realizacji w odniesieniu do kolejnych figur.

[0051] Figura 2 ukazuje w sposób schematyczny kolejność przeprowadzania dostępów do platformy centralnej oraz sporządzenie zapisanych tam danych i powiązań oraz manipulację nimi.

[0052] Platforma centralna według tego przykładu jest sporządzona w tradycyjnej architekturze MVC (Model-View-Controller). Użytkownik może uzyskać dostęp do platformy centralnej przez interfejs sieciowy, korzystając na swoim urządzeniu lokalnym z odpowiedniej przeglądarki. Interfejs sieciowy platformy centralnej jest dostarczany przez tradycyjny serwer sieciowy. Od płaszczyzny serwera sieciowego oddzielone są płaszczyzna danych i zastosowania zewnętrzne. Na płaszczyźnie danych są zapisywane dane, na przykład na tradycyjnym serwerze bazy danych (serwer SQL).

[0053] Na figurze 2, przez okres użytkowania pojazdu, który również w tym przypadku jest traktowany jako zespół fizyczny, od lewej do prawej strony pokazano kolejność dostępów podczas czasu funkcjonowania. Podczas produkcji najpierw to producent ma kontrolę fizyczną nad pojazdem. Producent ma w tym momencie również dostęp do platformy centralnej w celu wprowadzenia do pojazdu pierwszych wpisów. Sporządza on wpisy dla pojazdu oraz dla jego urządzenia kontroli dostępu (SID – Smart Identity Device) i sprzęga urządzenie kontroli dostępu z pojazdem. Dzięki temu sprzężeniu po stronie producenta wytwarzane zostaje utworzone niepowtarzalne i trwałe sprzężenie pomiędzy systemem pojazdu a SID. System pojazdu akceptuje odpowiednio rozkazy sterujące sprzężonego SID. Po wyprodukowaniu pojazdu i sprzężeniu go pojazd jest transportowany do sprzedawcy, co pokazuje figura 2.

[0054] Gdy tylko pojazd jest dostarczony lub przekany użytkownikowi, przez interfejs sieciowy na platformie centralnej sprzedawca tworzy tego użytkownika jako tożsamość i przenosi na platformie centralnej pojazd na użytkownika. Sprzedawca stwarza zatem sprzężenie pomiędzy pojazdem, przypisanym mu SID oraz stworzoną przez niego identyfikacją użytkownika

[0055] Następnie pojazd jest fizycznie przekazywany nowemu właścicielowi. Utworzony przez sprzedawcę właściciel dysponuje prawami, by w platformie centralnej ustanowić kolejnych użytkowników jako użytkowników pojazdu dla sprzężonych z nim pojazdów i SID-ów. Tym kolejnym użytkownikom, na przykład samemu właścicielowi lub członkom jego rodziny (ale także wynajmującym w przypadku zarządzania samochodami na wynajem), właściciel pojazdu może precyzyjnie przydzielać prawa za pomocą interfejsu sieciowego platformy centralnej. Poza tym właściciel pojazdu może zdecydować, który użytkownik może uzyskać dostęp do których praw za pomocą jakiego rodzaju środków identyfikacji oraz czy prawa te podlegają ograniczeniu czasowemu, zatem stają się nieważne w określonym momencie lub po wyznaczonym czasie. Chodzi przy tym o to, aby określić rodzaj i sposób, w jaki użytkownik za pomocą przenośnego urządzenia dostępu, w tym przypadku smartfona, może uzyskać dostęp do pojazdu. Właściciel pojazdu może w tym celu ustalić, że dla niektórych rodzajów dostępu i praw konieczne jest jedynie podanie numeru PIN, podczas gdy w przypadku innych praw (na przykład uruchomienia pojazdu) konieczne jest rozpoznanie danych biometrycznych (np. rozpoznanie twarzy lub rozpoznanie odcisku palca).

[0056] Pojazd może być wówczas przekazany przez właściciela pojazdu każdorazowo do użytkownika, co zostało przedstawione na figurze 2 jako prawa kolumna. Taki użytkownik pojazdu po zakończonej powodzeniem identyfikacji w platformie centralnej może na przykład za pomocą smartfona zapytać, jakie ma prawa w odniesieniu do określonego pojazdu, jednak nie może zmieniać tych praw.

[0057] Można zauważyć, że na różnych płaszczyznach przewidziano różne prawa do dostępu oraz do zmiany danych w platformie centralnej. Podczas gdy producent może zarówno utworzyć wpis dotyczący samochodu, jak również przypisanego mu SID oraz sprzęgnąć je ze sobą, sprzedawca nie może już wywierać wpływu na dane pojazdu oraz SID. Natomiast sprzedawca może utworzyć dla każdego pojazdu wpis dotyczący właściciela i sprzęgnąć go z istniejącymi już danymi pojazdu oraz SID. Właściciel może z kolei kontrolować, sporządzać i zmieniać prawa do pojazdu oraz tworzyć kolejnych użytkowników. Wreszcie użytkownik może jedynie sprawdzić swoje własne prawa w platformie centralnej.

[0058] Każdy z procesów przypisywania może być chroniony w myśl różnych pomysłów dotyczących bezpieczeństwa. W tym przykładzie wykonania podczas przypisywania pojazdu do właściciela pojazdu przez sprzedawcę zainicjowano na przykład taki następujący proces:

[0059] Jeśli sprzedawca wprowadza do platformy centralnej, że pojazd powinien zostać połączony z nowo sporządzoną tożsamością, najpierw w bazie danych zapisywane jest powiązanie, które sprzęga właściciela z pojazdem oraz przypisanym do pojazdu SID. Następnie używa się numeru telefonu komórkowego, zapisanego dla właściciela pojazdu, w celu wysłania przez platformę centralną wiadomości (na przykład SMS) na ten numer telefonu. Za pomocą tej wiadomości właściciel pojazdu jest informowany, że przypisano mu w platformie centralnej nowy pojazd. Wiadomość (na przykład znów SMS) jest poza tym wysyłana do sprzężonego SID przypisanego pojazdu. W tej wiadomości żąda się od SID (wywołuje się je), aby wysłał zapytanie do platformy centralnej w celu wywołania aktualizacji praw dostępu z platformy centralnej. Tego rodzaju wiadomości wywołujące są również stosowane, gdy przyznanie praw w odniesieniu do danego SID zostanie zmienione w pojeździe. Takie wywołanie jest pewniejsze niż bezpośrednie przesyłanie ustawień uprawnień, ponieważ manipulacja w przypadku wywołanego zapytania platformy centralnej

jest mniej prawdopodobna, niż gdyby przekazane dane SID zostały bezpośrednio zaakceptowane.

[0060] W tym przykładzie realizacji urządzenie SID poprzez odebraną wiadomość przyczynia się, aby utworzyć łącze danych z platformą centralną poprzez moduł GSM. Następnie na SID pobierane są zaktualizowane dane, włącznie z danymi odnoszącymi się do nowo utworzonego użytkownika. SID po stronie pojazdu koduje i zapisuje prawa dostępu dla użytkownika w urządzeniu. Łącze jest zabezpieczone dzięki sprawdzaniu certyfikatów, przy czym w SID zapisane są już po stronie producenta certyfikaty pochodzeniowe platformy centralnej.

[0061] W analogiczny sposób przyznanie praw może zostać przeprowadzone przez użytkownika dla jego pojazdu w późniejszym czasie. Gdy tylko użytkownik zmieni w platformie centralnej przyznanie praw do swoich pojazdów, platforma centralna wysyła do właściwego SID w pojeździe wiadomość, która wywołuje aktualizację przyznania praw w SID pojazdu.

[0062] Na płaszczyźnie użytkownika jest przy tym również możliwe, aby sprzęgać prawa dostępu z ustawieniami czasu lub okresem ważności, zatem przejściowe przydzielanie praw innym użytkownikom pojazdu. Przyznanie praw właścicielowi pojazdu następuje zasadniczo trwale, właściciel może jednak przekazać prawa użytkownikowi z ograniczeniem czasowym lub na pewne przedziały czasowe. Tego rodzaju ograniczenia czasowe są wówczas przekazywane przez platformę centralną do SID pojeździe i tam są również zapisywane w postaci zakodowanej. Na przykład można przewidzieć, że po upływie praw korzystania SID nie pozwoli na ponowne uruchomienie pojazdu lub mocno ograniczy prędkość maksymalną.

[0063] Poza tym zasadniczym przyznaniem praw w obrębie platformy centralnej oraz przekazaniem praw przez platformę centralną do SID pojazdu istotna jest także interakcja pomiędzy użytkownikiem a jego urządzeniem przenośnym, w szczególności smartfonem.

[0064] Na smartfonie wykonana jest aplikacja, która może przeprowadzić komunikację zarówno z platformą centralną, jak i z SID pojazdu. W tym celu aplikacja jest na przykład wgrywana przez sprzedawcę na urządzenie właściciela pojazdu lub aplikacje dla różnych systemów operacyjnych można pobrać z właściwych platform lub sklepów internetowych.

[0065] Przy pierwszym użyciu aplikacji na urządzeniu mobilnym użytkownik jest proszony o podanie nazwy użytkownika oraz hasła. Te dane są wykorzystywane w celu obliczenia wartości klucza haszującego, która jest przekazywana platformie centralnej. Komunikacja z platformą centralną może przy tym nastąpić za pomocą zwykłego trybu przekazywania, np. poprzez (zakodowany) protokół HTTP. Platforma centralna sprawdza, czy użytkownik istnieje w jej bazie danych, oraz oblicza także wartość klucza haszującego na podstawie zapisanych w platformie centralnej danych, dotyczących nazwy użytkownika oraz hasła. Wartość ta jest porównywana z przekazaną wartością klucza haszującego. O ile porównanie nazw użytkownika oraz wartości klucza haszującego daje pozytywne uwierzytelnianie, platforma centralna przekazuje aplikacji przypisane użytkownikowi SID-y oraz pojazdy. Te dane są zapisywane w sposób zakodowany przez aplikację na smartfonie w celu identyfikacji użytkownika.

[0066] Po stwierdzeniu, że użytkownik jest zasadniczo wiarygodny, w celu zabezpieczenia praw dostępu żąda się od niego nauczenia się różnych metod uwierzytelniania na smartfonie. W szczególności jest on proszony o podanie niepowtarzalnego numeru PIN, przeprowadzenie wzorcowego ruchu na wyświetlaczu smartfona oraz przeprowadzenie rozpoznawania twarzy lub rozpoznawania odcisku palca.

[0067] Te różne metody uwierzytelniania przedstawiają różne pewne stopnie dostępu do różnych funkcji pojazdu. To, które uwierzytelniania albo też sprzężenie których uwierzytelnień wystarcza do uzyskania dostępu do danej funkcji pojazdu, jest wprowadzane do platformy centralnej.

[0068] Następnie użytkownik aplikacji na smartfonie może w celu uzyskania dostępu aktywować po raz pierwszy jeden z pojazdów, który został zgłoszony przez platformę

centralną do aplikacji jako pojazd przypisany. Użytkownik wybiera pojazd do aktywacji, wysyła aplikacji zapytanie aktywacyjne do platformy centralnej, a platforma centralna tworzy przypadkowy kod, który jest ważny przez ograniczony czas. Ten przypadkowy kod aktywacyjny jest wysyłany osobną wiadomością na telefon komórkowy użytkownika. Musi on podać w aplikacji kod aktywacyjny z tej osobnej wiadomości, a aplikacja wysyła ten kod aktywacyjny z powrotem do platformy centralnej. W ten sposób zapewnia się to, że użytkownik rzeczywiście otrzymuje po drodze wiadomość, która jest zapisana w platformie centralnej.

[0069] Platforma centralna zatwierdza kod aktywacyjny i wysyła do aplikacji na smartfonie odpowiednie potwierdzenie. Aplikacja na smartfonie tworzy wówczas parę kluczy, utworzoną z klucza prywatnego i publicznego, i tworzy CSR (Certificate Signing Request), który jest wysyłany do platformy centralnej. Platforma centralna otrzymuje ten CSR i tworzy certyfikat X509 dla użytkownika oraz przypisane mu połączenie SID i pojazd. Oznacza to, że dla każdego użytkownika i każdego połączenia pojazd/SID jest tworzony certyfikat, który zawiera zarówno ID użytkownika, jak również identyfikator SID. Te dane o certyfikacie są z powrotem przesyłane do aplikacji na smartfonie, wraz z adresem Bluetooth SID danego pojazdu.

[0070] Te dane są odbierane przez aplikację i zapisywane w postaci zakodowanej. Aplikacja dysponuje wówczas adresem Bluetooth przypisanego SID, co pozwala na łączenie parami aplikacji na smartfonie z przypisanym SID przez Bluetooth.

[0071] Powyższy opis do tego przykładu wykonania opisuje wszystkie działania przygotowawcze, które trzeba przeprowadzić tylko raz lub w przypadku zmian praw dostępu. Częściowo te procesy należy przeprowadzić także wtedy, gdy właściciel pojazdu lub użytkownik pojazdu chciałby użyć nowego urządzenia przenośnego w celu uzyskania dostępu do istniejącego pojazdu.

[0072] W praktyce zdecydowanie najczęstszym przypadkiem jest codzienny dostęp do jednorazowo skonfigurowanego systemu w pojeździe. W tym celu pomiędzy aplikacją na urządzeniu mobilnym a SID w pojeździe tworzy się bezprzewodowe połączenie o małym zasięgu. Ten proces tworzenia par przebiega w znany sposób, ewentualnie na początku konieczne jest potwierdzenie sprzężenia obu urządzeń, co jest niezależne od rodzaju używanego systemu operacyjnego i ustawień na smartfonie. Jednak już przy aktywacji pojazdu i przypisanego mu SID smartfon otrzymuje dane adresowe SID w celu połączenia Bluetooth, tak że tego rodzaju potwierdzenie może również zostać pominięte.

[0073] Jeśli tego rodzaju tworzenie par jest przeprowadzone skutecznie, użytkownik przy otwartej aplikacji może uzyskać dostęp do funkcji pojazdu, na przykład przez interfejs graficzny, który jest pokazany na ekranie dotykowym smartfona.

[0074] Funkcje pojazdu mogą na przykład dotyczyć zamków drzwiowych, uruchamiania silnika, uruchamiania ogrzewania lub ogrzewania postojowego, otwierania okien, otwierania pokrywy tylnej lub włączania urządzeń oświetleniowych w pojeździe.

[0075] Figura 3a ukazuje na przykład przebieg dostępu, gdyby użytkownik chciał uzyskać dostęp do funkcji samochodu za pomocą swojego smartfona. Ten diagram należy czytać od góry do dołu.

[0076] Użytkownik otwiera na swoim smartfonie aplikację dostępu do pojazdu i wybiera polecenie w celu odblokowania drzwi. Aplikacja na smartfonie sprawdza na podstawie zapisanych danych, jakie uwierzytelnianie ze strony użytkownika jest wymagane dla tej funkcji i żąda je od użytkownika, o ile na tym etapie uwierzytelnianie nie zostało jeszcze podjęte przy uruchamianiu aplikacji.

[0077] Potem aplikacja stwierdza, że nie jest sprzężona z SID sterowanego pojazdu i najpierw tworzy połączenie w technologii Bluetooth z SID pojazdu. Poprzez połączenie Bluetooth ustanawiane jest pewne połączenie transmisji danych, zatem poprzez płaszczyznę protokołu mającą wyższy poziom niż Bluetooth. Wówczas aplikacja przekazuje do SID dyspozycję otworzenia drzwi. W tym przykładzie użytkownik nie jest jednak znany po

stronie SID (SID nie jest jeszcze aktywowane dla tego użytkownika). SID daje stosowną odpowiedź na telefon komórkowy, że użytkownik nie jest znany. W rezultacie aplikacja żąda od SID aktywacji użytkownika, po czym SID stawia zapytanie aktywacyjne do platformy centralnej poprzez moduł GSM. Platforma centralna daje SID potwierdzenie, że użytkownik jest wylegitymowany dla danego pojazdu i aktywował SID, i przesyła odpowiednie informacje o dostępie.

[0078] Potem SID daje telefonowi komórkowemu potwierdzenie aktywacji użytkownika. Aplikacja na smartfonie powtarza potem żądanie otworzenia drzwi, co jest potwierdzane za pomocą SID i ostatecznie drzwi są odblokowywane dla użytkownika. Opisany scenariusz dotyczy najgorszego przypadku, w którym przebieg może obejmować wszystkie pokazane kroki. Zazwyczaj jednak podczas zbliżania się użytkownika do pojazdu połączenie Bluetooth jest już utworzone, a użytkownik jest już także znany w SID. Wówczas proces przebiega przy znacznie mniejszej liczbie etapów i niezwykle szybko. Ten przebieg w zwykły rodzaj i sposób pokazano na figurze 3b.

[0079] Zgodny z wynalazkiem sposób postępowania umożliwia niezwykle pewne zarządzanie i elastyczne administrację prawami użytkownika, na przykład w taborze, jednak również przy użyciu innych zespołów fizycznych, np. maszyn lub tym podobnych. Dzięki oddzielnym kanałom komunikacji pomiędzy SID na każdym zespole fizycznym a platformą centralną z jednej strony oraz platformą centralną a urządzeniem przenośnym (smartfonem) z drugiej strony zwiększa się bezpieczeństwo. Dzięki temu, że poza tym użytkownik jest wzywany jeszcze do uwierzytelnienia na przenośnym urządzeniu dostępu, aby w ogóle móc uzyskać dostęp do zakodowanych danych zapisanych na urządzeniach przenośnych, dodawany jest kolejny stopień bezpieczeństwa.

[0080] Zakodowana pamięć w przenośnym urządzeniu dostępu (w szczególności smartfonie) zawiera na przykład informacje dotyczące aktywowanych pojazdów, informacje dotyczące SID sprzęganych z pojazdami, w szczególności ich adresy Bluetooth oraz kody połączeń, certyfikaty klienta i klucze do komunikacji, oraz listy metod uwierzytelniania w przypadku żądania dyspozycji, jak również informacje o użytkowniku, w szczególności nazwy użytkowników i hasła.

[0081] W pamięci SID zapisane są dla każdego pojazdu, na przykład w sposób zakodowany, prywatne klucze SID, certyfikat SID oraz certyfikat i/albo klucz publiczny platformy centralnej.

[0082] Zapisywanie danych w urządzeniach umożliwia elastyczny sposób kontroli dostępu. W szczególności informacje o certyfikacie zapisane w SID pojazdu mogą zostać wykorzystane do tego, aby za pomocą smartfona utworzyć tymczasową relację zaufania pomiędzy pojazdem a użytkownikiem żądającym dostępu. Aplikacja użytkownika, jak opisano powyżej, otrzymuje informacje o dostępie dla SID z platformy centralnej. Przy tym informacja jest kodowana za pomocą klucza prywatnego platformy centralnej. SID po stronie pojazdu zawiera informacje o certyfikacie głównych platformy centralnej. Nawet w przypadku, gdy SID nie ma dostępu do platformy centralnej, dzięki tej konstrukcji można każdorazowo zapewnić użytkownikowi tymczasowy dostęp do danego pojazdu. Mianowicie, jeśli SID może na podstawie zapisanych informacji na temat certyfikatów głównych pozytywnie zweryfikować to, że informacje przesłane smartfonem za pomocą aplikacji do SID zostały rzeczywiście zasygnowane przez platformę centralną, można utworzyć tymczasową relację zaufania. Jest to w szczególności istotne wtedy, gdy nowy użytkownik chce sobie zapewnić dostęp do wynajmowanego samochodu, jednak wynajmowany samochód znajduje się przykładowo w obszarze o słabym zasięgu telefonii komórkowej. Jeśli porównywanie certyfikatów w SID pojazdu jest zakończone powodzeniem, użytkownikowi może zostać przyznany dostęp do pojazdu, a pojazd zażąda pełnych praw użytkownika, gdy tylko pojawi się połączenie z siecią.

Zastrzeżenia patentowe

1. Sposób sterowania dostępem do urządzeń fizycznych,
przy czym każde urządzenie fizyczne jest wyposażone w jednostkę kontroli dostępu, która może blokować i odblokowywać dostęp do funkcji zespołu fizycznego,
przy czym stosuje się centralną platformę sterującą,
przy czym pomiędzy centralną platformą sterującą a jednostkami kontroli dostępu można ustanowić bezprzewodowe połączenia komunikacyjne,
przy czym występują przenośne urządzenia dostępu, które użytkownik może nosić ze sobą i które mogą tworzyć z jednostkami kontroli dostępu oraz centralną platformą sterującą bezprzewodowe połączenia komunikacyjne,
że przy dostępie użytkownika do urządzenia fizycznego przy użyciu przenośnego urządzenia dostępu przeprowadza się sprawdzanie tożsamości użytkownika, przy czym użytkownik identyfikuje się przed przenośnym urządzeniem dostępu,
przy czym po zakończonym powodzeniem sprawdzeniu tożsamości ustanawiane jest bezprzewodowe połączenie komunikacyjne pomiędzy przenośnym urządzeniem dostępu a jednostką kontroli dostępu urządzenia fizycznego,
przy czym do jednostki kontroli dostępu przesyła się przez przenośne urządzenie dostępu co najmniej tożsamość użytkownika oraz niepowtarzalne dane dotyczące dostępu,
znamienny tym,
że jednostka kontroli dostępu określa prawa dostępu do urządzenia fizycznego i przyznaje je użytkownikowi na podstawie otrzymanych informacji oraz na podstawie kolejnych informacji, które jednostka kontroli dostępu otrzymuje od centralnej platformy sterującej,
przy czym po otrzymaniu informacji od przenośnego urządzenia dostępu jednostka kontroli dostępu sama wysyła do centralnej platformy sterującej informacje dotyczące tożsamości użytkownika oraz niepowtarzalnego identyfikatora jednostki kontroli dostępu przez bezprzewodowe połączenie komunikacyjne, następnie centralna platforma sterująca ustala prawa dostępu zidentyfikowanego użytkownika do zespołu fizycznego, przypisanego jednostce kontroli dostępu, a centralna platforma sterująca przekazuje uprawnienia dostępu przez bezprzewodowe połączenie komunikacyjne do jednostki kontroli dostępu i jednostka kontroli dostępu na podstawie tych informacji udziela prawa dostępu.

2. Sposób według zastrzeżenia 1, przy czym jednostka kontroli dostępu przekazuje do centralnej platformy sterującej także informacje dotyczące niepowtarzalnego identyfikatora przenośnego urządzenia dostępu.

3. Sposób według zastrzeżenia 1, przy czym jednostka kontroli dostępu poza tym niezależnie od dostępów użytkownika, otrzymuje i zapisuje w odstępach czasowych informacje od centralnej platformy sterującej,
przy czym na podstawie tych zapisanych informacji oraz informacji otrzymanych od przenośnego urządzenia dostępu jednostka kontroli dostępu, podczas próby dostępu, ustala i zapewnia prawa dostępu.

4. Sposób według jednego z poprzednich zastrzeżeń, przy czym identyfikacja użytkownika przed przenośnym urządzeniem dostępu następuje na podstawie danych biometrycznych, w szczególności przez przeprowadzenie rozpoznawania twarzy i/albo przez przeprowadzenie rozpoznawania głosu i/albo rozpoznawania odcisku palca.

5. Sposób według jednego z poprzednich zastrzeżeń, przy czym przenośne urządzenie dostępu jest implementowane w przenośnym urządzeniu komunikacyjnym, w szczególności smartfonie, na którym wykonywana jest aplikacja, która przeprowadza sprawdzanie tożsamości oraz komunikację pomiędzy urządzeniem komunikacyjnym a jednostką kontroli dostępu.

6. Sposób według jednego z poprzednich zastrzeżeń, przy czym pomiędzy przenośnym urządzeniem dostępu a centralną platformą sterującą jest ustanawiane połączenie komunikacyjne, przy czym centralna platforma sterująca przekazuje do przenośnego urządzenia dostępu informacje o certyfikacie, przy czym informacje o certyfikacie są każdorazowo przypisywane tożsamościom użytkownika.

7. Sposób według zastrzeżenia 6, przy czym pomiędzy jednostką kontroli dostępu a centralną platformą sterującą jest ustanawiane połączenie komunikacyjne, przy czym centralna platforma sterująca przekazuje do przenośnego urządzenia dostępu informacje o certyfikacie do zapisania, które umożliwiają sprawdzanie autentyczności i integralności informacji, które są przekazywane przez przenośne urządzenie dostępu do jednostki kontroli dostępu.

8. Sposób według zastrzeżenia 7, przy czym centralna platforma sterująca przekazuje do przenośnego urządzenia dostępu potwierdzenie tożsamości, przy czym co najmniej jedna część potwierdzenia jest zakodowana kluczem prywatnym centralnej platformy sterującej,
przy czym jednostka kontroli dostępu otrzymuje od centralnej platformy sterującej klucz publiczny, za pomocą którego mogą zostać zweryfikowane informacje o tożsamości uzyskane przez przenośne urządzenie dostępu.

9. Sposób według jednego z zastrzeżeń 6do 8, przy czym informacje o certyfikacie przekazane do przenośnego urządzenia dostępu przez centralną platformę sterującą są zaopatrzone w informacje o upływie czasu, które podają czas ważności certyfikacji.

10. Sposób według jednego z poprzednich zastrzeżeń, przy czym jednostka kontroli dostępu, gdy nie można ustanowić komunikacji danych z centralną platformą sterującą, weryfikuje ważność certyfikatu z transmisji z przenośnego urządzenia dostępu za pomocą zapisanych danych, a w przypadku ważnego certyfikatu zapewnia zidentyfikowanemu użytkownikowi ustalony wybór praw dostępu.

11. Sposób według zastrzeżenia 10, przy czym wybór praw dostępu zezwala na ograniczone korzystanie z zespołu fizycznego, w szczególności ograniczenie czasowe albo funkcjonalne.

12. Sposób według jednego z poprzednich zastrzeżeń, przy czym jako urządzenia fizyczne stosowane są pojazdy.

13. Sposób według jednego z poprzednich zastrzeżeń, przy czym dla każdego połączenia użytkownika i zespołu fizycznego jest sporządzany niepowtarzalny certyfikat, który jest zapisywany w przenośnym urządzeniu dostępu.

14. Sposób według jednego z poprzednich zastrzeżeń, przy czym centralna platforma sterująca dla każdego zespołu fizycznego zapisuje niepowtarzalny adres przypisanej jednostki kontroli dostępu w celu utworzenia bezprzewodowego połączenia o małym zasięgu, w szczególności połączenia Bluetooth, i przesyła ten adres do przenośnego urządzenia dostępu.

Uprawniony: **Huf Hülsbeck & Fürst GmbH & Co. KG**

Pełnomocnik:

mgr inż. Marta Skrobot
Rzecznik patentowy

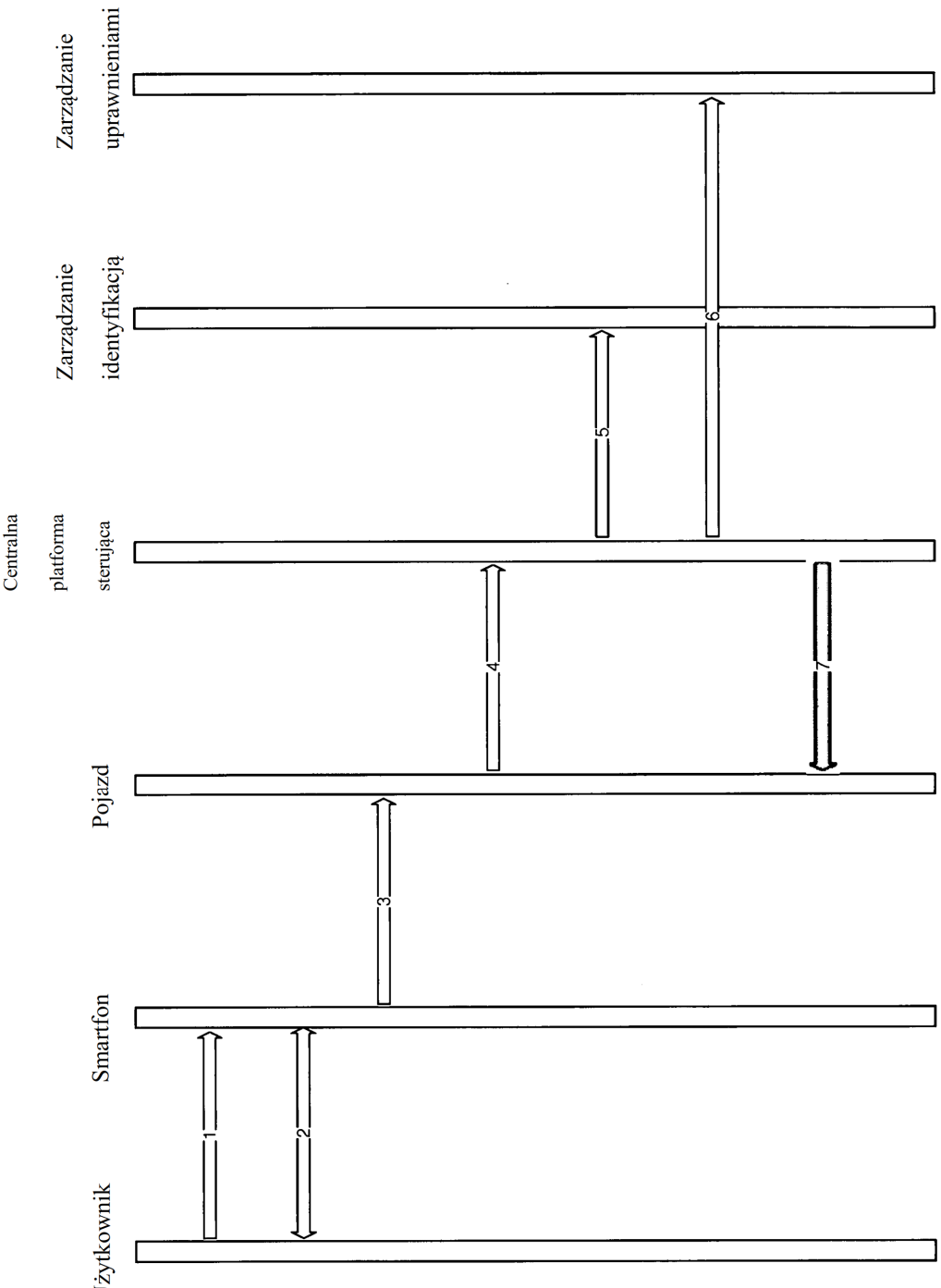

Użytkownik
Smartfon
Pojazd
Centralna platforma sterująca
Zarządzanie identyfikacją
Zarządzanie uprawnieniami
1
2
3
4
5
6
7

Fig. 1

Fig. 2

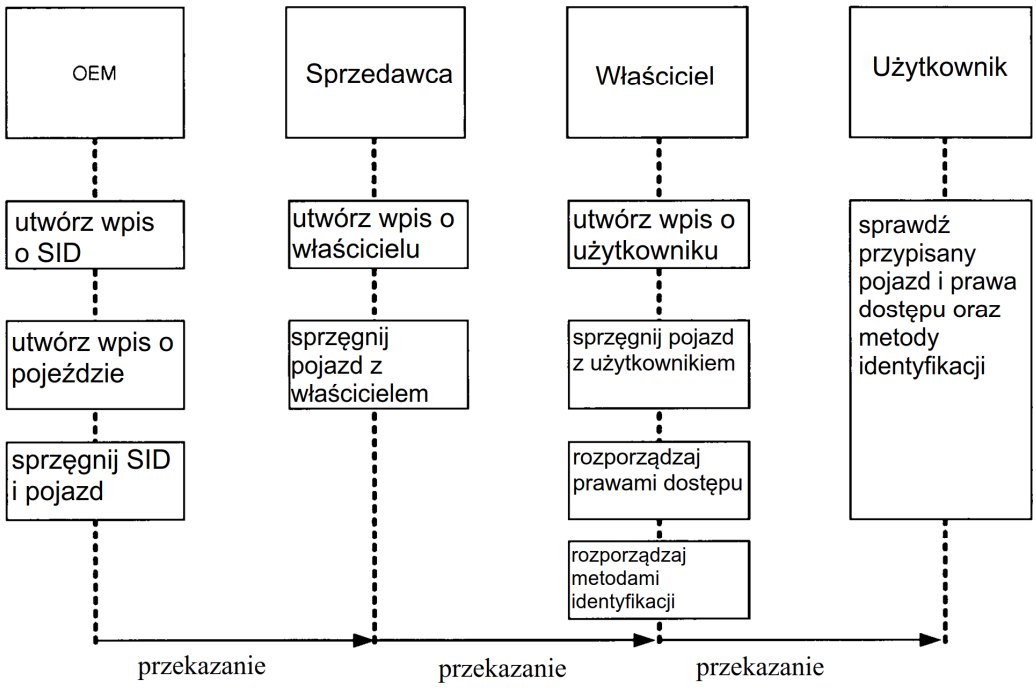

OEM
Sprzedawca
Właściciel
Użytkownik
utwórz wpis o SID
utwórz wpis o pojeździe
sprzęgnij SID i pojazd
utwórz wpis o właścicielu
sprzęgnij pojazd z właścicielem
utwórz wpis o użytkowniku
sprzęgnij pojazd z użytkownikiem
rozporządzaj prawami dostępu
rozporządzaj metodami identyfikacji
sprawdź przypisany pojazd i prawa dostępu oraz metody identyfikacji
przekazanie
przekazanie
przekazanie

Fig. 3a

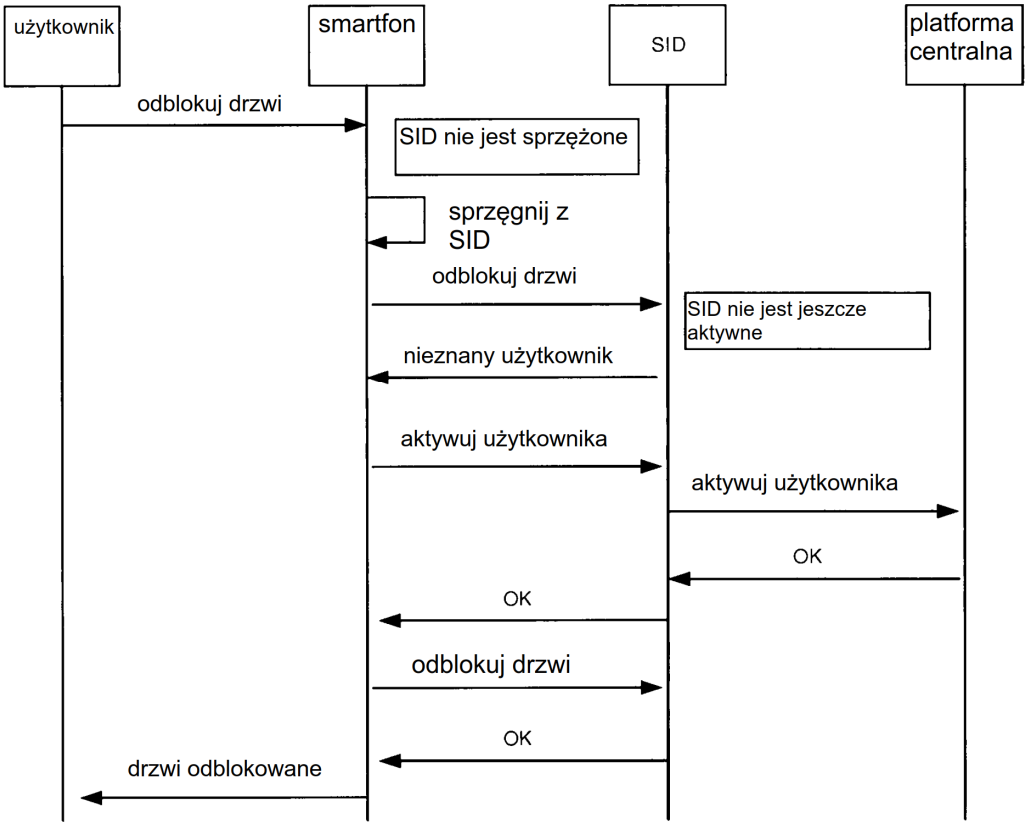
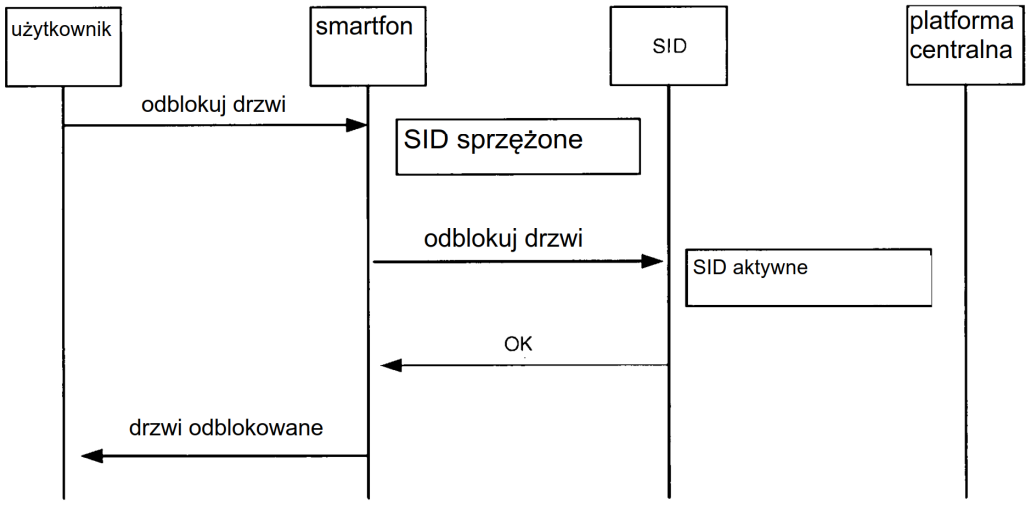

użytkownik
smartfon
SID
platforma centralna
odblokuj drzwi
SID nie jest sprzężone
sprzęgnij z SID
odblokuj drzwi
SID nie jest jeszcze aktywne
nieznany użytkownik
aktywuj użytkownika
aktywuj użytkownika
OK
OK
odblokuj drzwi
OK
drzwi odblokowane

Fig. 3b


użytkownik
smartfon
SID
platforma centralna
odblokuj drzwi
SID sprzężone
odblokuj drzwi
SID aktywne
OK
drzwi odblokowane