(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 February 2015 (12.02.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/019104 A2

(51) **International Patent Classification**:
G07C 9/00 (2006.01)

(21) **International Application Number**:
PCT/GB2014/052429

(22) **International Filing Date**:
7 August 2014 (07.08.2014)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:
1314172.6 7 August 2013 (07.08.2013) GB

(71) **Applicant**: **EUS ASSOCIATES LTD** [GB/GB]; 4 The Rowans, Saxilby, Lincoln LN1 2SP (GB).

(72) **Inventors**: **GREAVES, Michael James**; 9 Connaught Avenue, Ashford Kent TW15 3HY (GB). **SHAW, Philip Martin**; 4 The Rowans, Saxilby, Lincoln Lincolnshire LN1 2SP (GB).

(74) **Agent**: **LOVEN PATENTS & TRADEMARKS LIMITED**; 3 Checkpoint Court, Lincoln Lincolnshire LN6 3PW (GB).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) **Title**: ACCESS AND CONTROL AUTHORISATION SYSTEM

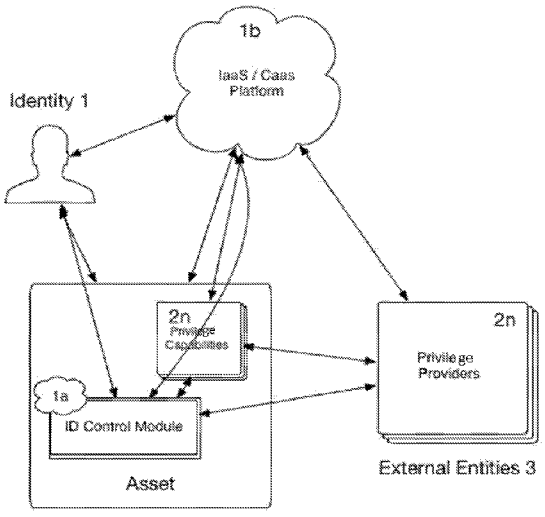


Fig 1

(57) **Abstract**: An access authorisation system comprises a central authenticator and an access device controlling access to each of a plurality of resources, the access device being remote from the central authenticator and being programmable and configured to communicate therewith. The authenticator stores: for each of a plurality of users, a user identifier and user identity data as- sociated therewith; for each of a plurality of access devices, an access device identifier and data relating to each of the resources controlled by the access device; and at least one privilege granted to each user to use at least a selected one of the plurality of resources controlled by at least one of the access devices. The authenticator and the access device are programmed to perform the following steps in response to the user requesting from the authenticator exer¬ cise of the privilege: (a) in response to receipt of the request, the authenticator requests the user to provide to the authenticator individual identifying data for the user; (b) the authenticator compares this with stored data to verify the user's identity; (c) the authenticator transmits to the access device instructions to allow the user to exercise the or each privilege.

WO 2015/019104 A2

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

ACCESS AND CONTROL AUTHORISATION SYSTEM

Field of the Invention

[0001] This invention relates to an access and control authorisation system.

Background to the Invention

[0002] The increasing use of microprocessor-based control and monitoring systems in conjunction with portable devices such as mobile telephones (cell phones) creates greater opportunities for abuse for criminal or malicious purposes. One area of concern is the automotive field, where the greater use of telematics for such purposes as vehicle tracking, remote diagnostics, fleet management or digitally-enabled services could potentially give rise to threats to vehicles or their users. For example, by linking vehicle system management computers to communications for reporting vehicle operations parameters, the risk is introduced of malicious interception of the communications for the purpose of adversely affecting the operation of the vehicle, theft of data, personal information or physical property within the vehicle.

[0003] In addition, access to the operation of vehicles and vehicle security and entry/usage authorisation is currently based on physical keys in locks, or tokens wirelessly communicating with the vehicle systems. In either case, possession of the key or token is all that is needed to allow use of or access to the vehicle and its subsequent control or access to its physical or logical systems or logical systems it may be able to present. It would be advantageous to be able to control use of a vehicle (or indeed other asset) through a device carried by the user that is not permanently linked to the vehicle or other asset, for example a smart phone, mobile telephone or cell phone, with use rights being transmitted centrally to the user's device and to the vehicle or asset so that the vehicle or asset can recognise the user's device as granting access or other rights when in communication there with. Also, it would be advantageous to provide a system whereby an individual can gain access to an object and its physical and logical assets with no token of authentication or authority other than himself. Further to this, it would be desirable to provide the ability within a particular

physical asset or system to grant control of access physically to itself or its physical or logical subsystems to a particular individual without the requirement for a physical authentication token or a Smart Phone software application operating as an authentication token or a discrete token for authentication or access (such as smart card or smart key).

[0004] More generally, there is a need to be able to communicate more securely with remote devices such as mobile telephones or vehicle telematics systems or off-board digital services to minimise the risk of unauthorised operations.

[0005] US2009/018541A1 discloses triangular communication to authenticate the user via his mobile phone and to grant access to a master locking device.

Summary of the Invention

According to one aspect of the invention, there is provided an access authorisation system comprising a central authenticator and an access device controlling access to each of a plurality of resources, the access device being remote from the central authenticator and being programmable and configured to communicate therewith, wherein the authenticator stores:

for each of a plurality of users, a user identifier and user identity data associated therewith;

for each of a plurality of access devices, an access device identifier and data relating to each of the resources controlled by the access device; and

at least one privilege granted to each user to use at least a selected one of the plurality of resources controlled by at least one of the ac-cess devices;

wherein the authenticator and the access device are programmed to perform the following steps in response to the user requesting from the authenticator exercise of the privilege:

(a) in response to receipt of the request, the authenticator re-quests the user to provide to the authenticator individual identifying data for the user;

(b) the authenticator compares the sent data with stored data to verify the user's identity;

(c) the authenticator transmits to the access device instructions to allow the user to exercise the or each privilege.

[0006] The user may be a person or an inanimate object having some form of processing and communication capacity. Where the user is a person, the authenticator is preferably programmed in step (a) to request the user to provide personal identifying data, which can comprise one or more of a personal identification number and unique physical characteristics of the user. The unique physical characteristics may include a fingerprint, a retina pattern, a face image or part thereof, and a speech sample, but are not limited to these, and can be anything which uniquely identifies an individual.

[0007] Preferably, the system further comprises a user device remote from the central authenticator and programmable and configured to communicate with the access device and with the central authenticator, wherein the user device, the authenticator and the access device are programmed to perform the following steps in response to the user causing the user device to request from the authenticator exercise of the privilege:

(a1) in response to receipt of the request, the authenticator instructs the user device to display to the user a request to input personal identity data;

(a2) the user device transmits the personal identity data input by the user to the authenticator and the authenticator compares this with stored data to verify the user's identity;

(a3) the authenticator transmits a transaction token to the access device and to the user device;

(a4) the user device communicates with the access device to request exercise of the privilege, the communication including the user device transaction token; and

(a5) a matching operation is performed on the user device transaction token and the access device transaction token and the access device is arranged to allow exercise of the or each privilege if the result of the matching process meets predetermined criteria.

[0008] Another aspect of the invention provides a secure communication system between a verification device and a remote device, wherein

the remote device comprises:

communication means for transmitting data to and receiving data from the verification device

processing means having an operating system for controlling the basic operation of the remote device and a container program installed thereon to function under the operating system,

the verification device comprises:

communication means for transmitting data to and receiving data from the remote device;

processing means programmed to communicate with the container program in the remote device to install on the remote device in response to receipt of a communication request from the remote device a temporary virtual machine controlling communication with the verification device independently of the operating system of the remote device;

and the container program is configured to uninstall the virtual machine from the remote device in response to an instruction from the verification device via the virtual machine.

[0009] The remote device may be the user's mobile telephone, and it will be appreciated that verification of the user can involve any of the features of a so-called smart phone, for example the use of a touchscreen, camera or microphone, or any combination of these. The use of a camera permits the application of close proximity gestures instead of, or as well as, the touchscreen. Other communication devices, for example wearable devices, may be used, paired with, or independently of, a smart phone.

[0010] The invention also provides a secure data communications system, comprising first and second programmable devices configured to communicate with each other and with a remote server device configured to issue at intervals to the first device and the second device an encrypted security code, the system further being configured such that, when any of the devices initiates communication with any of the other devices by transmission of its security code,

the receiving device compares the received code with the most recent security code received from the server and only allows communication to continue if the conformity between the codes and their transmission criteria is within predetermined limits.

[0011] In a vehicular context, upon successful authorisation to gain access to and initiate a driving session the person enacting such privileges is viewed as a "Connected Driver", being by request and consent authorised to control a vehicle and by doing so is bound by the laws and regulations required.

[0012] Other features of the invention are set out in the claims.

[0013] The following is the composite list and description of elements to create the end to end system that will deliver the method.

Internet Cloud Based Service Engine – The Platform

[0014] The Platform is a multi-tiered "wholesale" architecture allowing diminishing grant of authority and administration. The prime function is to deploy white label sub instances that can be separately branded upon which a customer bespoke market can be created with the SDKs and APIs provided.

Secure Mobile Engine

[0015] A proprietary software system for securely delivering real-time customized applications, built within the rules of The Platform, to common portable internet devices (iPhone, Android, Microsoft Windows Mobile, Blackberry or a WC3 compliant mobile browser). The software system does not create an installed application onto a portable device but instead delivers a facsimile of a mobile application within a secure container. The system leaves no residual transactional data on the portable device, other than that which is required for facilitation of the visuals of an application once the app is closed or a specific function has been achieved. The content off the applications is based on composite elements of services and functionality borne from The Platform. Any standard industry security technology can be applied to the transmission path between the platform and the display within the connected handheld device. The system also allows control and effect of hardware and API elements within

the internet device, for example the ability to enable GPS, Bluetooth, and a camera function. The system is however not a "web app" as access is through a proprietary software container rather than the generic device web browser.

Endpoint Gateway Application

[0016] This is a proprietary embedded software application typically within an open standard operating environment (e.g., Java, Android) that is effectively a remote agent of The Platform at the vehicle or secured object. This object (software or software within a device) controls a physical locking mechanism and capability to allow access to connected downstream subsystems. This element may be represented by either a black box containing a controller chip with an embedded operating system (Java, Android etc.) or expressed as an application the function of which can function on a number of open standard embedded operating systems. The functions of this software are –

a) To provide a receptacle for the Secure Mobile Engine,

b) As agent software in which to deploy secure data via the mobile application fabric from within the platform.

c) To allow instructions from The Platform to parse encrypted or open messages to a vehicles systems or subsystems, for example, "open doors", "lock doors", "disable immobilizer", "start engine" via an API. Similarly, the vehicle can present subsystem messages to the vehicle gateway application to be encoded and sent to The Platform for processing, encapsulating within a context and publishing for availability is systems or services within The Platform or available to eternal applications or databases.

d) To act as a security gateway, firewall and single point of ingress for external data communication to subsystems, IVI, critical safety systems, telematics data and functional system data (e.g., engine warning lights).

[0017] The Gateway Application operates in two modes: Online, where there is access to external internet based services via public wireless networks via the host iteration of The Platform; and an Offline mode, where a perpetuating recursive logic system maintains vehicle system and subsystem security as well

as condition grant of access and use for validated and authorized drivers or those requiring access to the vehicle and sequential validated access to sub systems and functions.

[0018] An additional function of the gateway is to provide an authenticated identity information path back through The Platform to off board web services (Twitter, Facebook etc.) and in doing so provides a "Single Sign On" facility for providing inbound web services or elements of web services into the higher functions of the car (e.g., the IVI or "head unit" display and its operating system). This allows prevention of the current issue of remnant services being retained in the vehicle (such as Satnav history, telephone records etc.), as each authenticated driver would see only their personal information rather than that of the previous driver/s.

[0019] Advantages of various aspects of the invention include:

i. Providing irrefutable proof of identity of a person wishing to access an object and control elements within that object in context to their identity and their privileges in context to that system in real-time taking theoretically a limitless number of external contributing factors to that permission being granted.

ii. The ability to identify uniquely all occupants of a vehicle or building and potentially retains records of that entry scenario and context.

iii. Disambiguating the notion of a lock and key, or key token with the metaphorical "unlocking" process being abreacted to The Platform or proactive decision making by elements granted into the asset end point. This makes theft or fraudulent entry to the system protected significantly reduced if not negated. In the case of vehicles, if the system were overcome then the control software in the vehicle would have based upon rules the possibility to render the car inoperable once the engine had been turned off etc.

iv. Removing entirely the requirement to have a physical key (electronic or mechanical), smart card or entry token.

v. Providing a novel method of delivering secure data to a mobile internet device regardless of operating system, installing no viable recoverable data in that device in case of loss and subsequent hacking

vi. If mobile data networks are not visible or out of coverage, the software within the protected system or object goes into offline mode deploying a time based unlock circulating code known only to that element and The Platform. Once an accredited person requires access, the reciprocal code is passed to the phone or device for the correct level of access and utilization. Once both the gateway and the handheld internet device are back in coverage, the normal process of real-time platform access falls back into place. Other systems offering a lock or unlock via mobile app do not address this problem.

vii. The capability to augment a potential flaw in the E-Call initiative and comparable initiatives in other territories, such as the USA. E-Call is a European wide automotive automatic call to emergency services in the event of an accident. This call is proceeded by a telematics data burst of location and other vehicle attributed to the emergency services. With our system in place, there is the capability to continue to send location and situational data (many mobile networks will not allow simultaneous voice and data connections). Therefore with a tertiary data connection, via The Platform, it will be possible to send continuous data relating to the situation, including for example vital signs indication, and link that situation to not just emergency services but also via the Platform, that knows categorically who is driving the car, and can provide access to medical records, insurance and recovery details, as well as information relating to the driver's friends, family, employer etc.

[0020] The invention therefore further provides a system installed in a vehicle comprising means for detecting vehicle criteria indicating the occurrence of an accident, secure transmission means for transmitting to a central controller remote from said vehicle in response to detection of said criteria data identifying at least one or more occupants of the vehicle. Preferably, the vehicle includes vital signs detection means for detecting indications that one or more of the oc-

cupants is alive, for example detecting sounds, CO_2 measurements indicating breathing, heartbeat monitor and eye movement monitor. The central controller may be configured to communicate relevant data to emergency services. The system is preferably associated with an E-Call or comparable installation in the vehicle, but capable of communicating independently of this.

Brief Description of the Drawings

[0021] In the drawings, which illustrate exemplary embodiments of the invention:

Figure 1 is a diagrammatic representation of a first embodiment of the invention;

Figure 2 illustrates the capability to create subordinate users and privileges relates thereto;

Figure 3 illustrates the use with the system of the first embodiment of a reprogrammable trust token;

Figure 4 illustrates another physical method of asserting an identity in relation to requesting or enacting a privilege;

Figure 5 is a hierarchy model illustrating a possible application of the system of the invention to a typical automotive case use;

Figure 6 is diagrammatic representation of an alternative embodiment of the invention; and

Figures 7 to 10 illustrate an example of the alternative embodiment, applied to controlling access and use of a motor vehicle.

Detailed Description of the Illustrated Embodiment

[0022] Figure 1 provides a topographical logical system overview. Identity 1 represents the irrefutable capture and encoding of an individual for use within the system. This may be captured using any relevant technology and will incorporate at least one biometric imprint encoded into the Identity 1 cryptographic file. 1a relates to a system control module or "SAM" Security Access Module (software or hardware implementation) that is contained within a tangible and physical asset. In an automotive context, this asset would be a car or vehicle. Contained within the capabilities of that asset is 2n, a manifesto of all software

and hardware capabilities requiring privilege grant that can be enacted and controlled by the overall system. 2n is synchronised between internal privilege capabilities and the providers and controllers of these privileges that exist externally to the physical asset. An individual will be required to have a relationship, contract, license or rights of use with an external Privilege Provider in order to activate a specific privilege function within an asset. For example, within an automotive context, an individual may have purchased the right to additional performance functions of a vehicle (e.g., higher engine power mapping and enhanced suspension damping) or access to specific software service available within the vehicle. These functions are controlled and provided externally to the vehicle.

[0023] The ID Control Module (SAM) operates in a connected, semi connected / autonomous or autonomous manner. Since encrypted privileges strings relating to a User Identity and associated Privileges are optionally stored resident within the SAM memory, the SAM can, based upon simple rules algorithms grant control of Privilege functions without the requirement of communicating directly with the Platform. Depending upon the environmental and contextual nature of the request, and based upon the rules model agreed between the SAM and the Platform, the SAM can grant conditional, temporary or limited grant of privilege without the requirement to verify the action from the Platform or from Privilege Providers. This for example would be deployed in a scenario where the SAM and asset do not have sufficient access to communication technologies to verify the validity of a request to enact a privilege. Once the Asset and the SAM regained access to communication with the Platform and Privilege Provider ecosystem the temporary or conditional grant of privilege could be confirmed, further limited or rescinded as appropriate. Similarly, even during good communication between all relevant elements, a Privilege can be revoked, redefined or limited dynamically depending upon the requirements or standing of the User enacting a specific Privilege.

[0024] 1b is a SOA based service platform comprised of "off the shelf" middleware components. Its prime function is to offer "IaaS" – Identity as a Service and "CaaS" – Context as a Service. A software service platform managing the

relationship between the application of a verified Identity in Context to services offered by an asset relating to the privileges available, paid for and or licensed to an Individual. E.g., in an automotive context, an individual may have the privilege of unlocking the doors, entering the vehicle and starting the engine. 1b is the primary management and verification system that links the disparate elements to create the context of a valid and authenticated usage of a privilege.

[0025] Because the functions for a specific Individual are synchronised between the asset, the platform and the providers, persistent verification of all elements of the architecture is required to fully enact specific privileges. However, the ID Control Module has the capability to autonomously take rules engine based decisions on temporary granting of privilege rights in a scenario where communications are not available for end to end messaging and verification between required entities or databases.

[0026] The system has been created not to simply provide physical access but in this context Access relates to the access of control of mechanical or digital and "connected" functions or services contained within the subject asset of the system. For example, this can mean to both unlock, but also lock and place a lock in a conditional state whereby the requirements and context for operation is defined by Identity 1, subordinate users, Identity n or is subject to the real time controls available to off-board Privilege Providers.

[0027] Figure 2 illustrates the capability for Identity 1 or the prime controller or user to create subordinate users. These users Privileges will be confined to within those of Identity 1 but also in relation to privileges available to Identity n based upon the privileges to which they have right to via Privilege Providers. Identity 1 also has the ability to create and federate sub-privileges and condition of privilege enactment to Identity n. This is further illustrated by the sample hierarchy model described in Figure 5 that is a sample model to cover a generic Automotive Hierarchy and Privilege management use case.

[0028] Referring to Figure 3, in addition to the ability to create hierarchical subordinate users, the system would allow the implementation of a reprogrammable trust token, possibly referred to as a "smart key" to act as a physical rep-

resentation of a User's ability to enact privileges. The privilege and rights programmed into this device would be granted and controlled by both Identity 1 but also on the basis of the relationship in dynamic contextual real time that Identity n has with Identity 1 and the functions granted in relation to any Privilege Providers from which Identity 1 or Identity n procures a Privilege service from. For example, Identity 1 could create an asset usage profile and embody that within a Trust Token that would be physically held by an assigned Identity n or multiple Identity ns. Each token would grant privileges specific to that Identity or individual. If Identity n attempts to illicitly enact a privilege outside of terms of that privilege grant, logic and rules within the Platform and ID Control Module (SAM) would reject the attempt. An example could be that Identity n has controlled access to an Asset only during business hours. An attempt to access certain Privilege functions outside of business hours would be rejected. In an Automotive context, this could relate to a commercial vehicle where the User / Identity n only has a contract to drive the vehicle during business hours and access relates to his specific Trust Token. Identity 1 can however conditionally and / or temporarily override or redefine that specific Identity n's Trust Token or apply rules of contextual conditionality as required.

[0029] Figure 4 illustrates the physical method of asserting an Identity in relation to requesting or enacting grant of a privilege can be delivered in multiple ways. An obvious method would be the use of a Smart Phone or similar Internet Enable Device. This device could be utilised as a tool to enter an authentication request be it, alpha numeric, Biometric, gesture based or combinatorial. The precise method or requirement would depend upon the device being used as well as the ad hoc contextual requirements demanded from the Platform, the requirements of the Privilege Providers or indeed the in asset SAM. Additionally we have covered the physical Trust Token model in Figure 3 however, verification of the Identity of the person holding or attempting to use that Token to validate a request could be enabled via this method, in particular if there is an element of doubt relating to the validity of the person in possession of the Trust Token.

[0030] There is also the possibility to provide Authentication via the latent capabilities or sensors within an Asset. Within an automotive context, this could mean the biometric verification utilizing an onboard camera or by embedding a touch pad or key pad into the external body or glass of the vehicle, as well as further verification and identity affirmation measures within the vehicle. More simplistic authentication could be deployed externally to the vehicle, but access to more critical systems (such as start engine, engage gear). The core principle of this mode is that physical access to an Asset and enactment of Privileges does not rely upon a Token, device, agent or App but solely upon the verification of the identity of Identity 1 or n which in collaboration with other contextual factors can provide an extremely high probability of a valid Privilege enactment or session.

[0031] Figure 5 is a hierarchy model denoting a possible process of precedence in a typical automotive use case for the system. It takes into account the technical prioritisation of control of the system elements as well as the commercial/financial ecosystem in the entire usage cycle of a typical vehicle whether privately owned, leased, daily rental or pool car. As such is an archetype model to map or accommodate all users within the majority of scenarios.

[0032] Referring now to Figure 6, the overall objective of the system of this embodiment is to provide a secure identity and access management solution that can be employed to provide a mobile user with access to a resource or an asset based upon a range of externalized privileges. Whilst the intention is that the solution should be usable to support a range of possible applications, the sample application defined in this document is based around a vehicular system and ecosystem.

[0033] The fundamental principle is that a irrefutably identified User Identity should be able to gain authenticated access to a resource, in such a way that the privileges associated with the User should be exposed to the resource to permit access control decisions. There is nothing particularly unique about this specific requirement – it corresponds to most common access control systems. However, the intention is that there be loose coupling between the components,

such that the resource manager does not require pre-knowledge of either the User or the privileges granted to the User. Additionally, the prime User or asset controller has the ability to create subordinate or even orphan users with their own access and privilege ecosystem in respect of access and usage rights to the asset in question.

[0034] The principle concept applied is the same as that associated with the Capability-Based security model, which in turn is a standard model for secure computing. The proposed design is an extension of the Capability-Based model to support a distributed computing architecture.

[0035] The role of the platform is to act as a trusted third party. It is used to register the identity of Users and SAMs – issuing them with identity credentials to support mutual identification. The platform also grants privileges to Users and provides this information to the App. The nomenclature applied to this, in this context is "IaaS" being Identity as a Service and "CaaS" being Context as a Service. The Platform is a generic Service Platform comprised of "off the shelf" databases, middleware and software but built and configured to deliver and manage the relationships and functions specific to this model.

SAM (Smart Access Module)

[0036] The SAM manages access to resources. It is able to authenticate its identity (using a credential issued by the platform) and mediate access to the resource using privilege information presented by the App (on behalf of the user), or other methods utilised to authenticate a Privilege assertion on or within the functions of the Asset. These other methods may include asset onboard biometric assertion and verification, alpha numeric ID assertion or a reprogrammable physical token of access such as smart card, key or object.

App

[0037] The App is a mobile device application. It provides a user interface to allow interaction between the User and Platform, as well as the User and SAM. The App also acts as a repository for User identity credentials and privilege information (issued by the Platform). The App can also be used to provide subor-

dinate privilege to additional users or to modify or acquire privileges held by an authenticated User Identity.

Asset / Resource

[0038] This can be any asset, tangible or not which requires assertion of an irrefutably identified User in order to provide privileges. For the purposes of this document, an example asset would be a vehicle. A privilege would be the right to unlock the doors or further to enable or disable any possible function within that vehicle depending upon the privilege rights of the identified user. Such functions could include but are not limited to physical security, selective physical security, activating the ignition, starting the engine, engaging gear, releasing the handbrake, the performance characteristics of the vehicle, access to physical functions available within the vehicle such as suspension settings, access to "sport" or other modes, access to content and functions of the In Vehicle Infotainment and Navigation systems or content and applications provided by external 3rd parties to which the identified User has an external privilege to access. Assets or Resources would be enrolled additionally as Identities in their own right. As such, an asset or resource would be able to access or control other resources or assets based upon its privileges within the architecture, thus allowing both instructed and automated interaction with other assets or devices.

Design Principals and Assumptions

[0039] The key design principles are:

- The SAM does not require pre-knowledge of the identity of users or their privileges.
- A SAM may be a physical element comprising electronic communication equipment, memory, a CPU and I/O capabilities to enact its function or it may be reference software that exists within a piece of specific hardware designed to enact its functions within a specific environment or asset.
- There may be an infinite set of users with privileges over the resource that the SAM is managing without any impact on the SAM.

- Resources (SAMs) may be added or removed without any impact on Users.
- The Platform provides identity and privilege credentials to SAMs and Users, such that these may be used to create mutual trust (authentication) between SAMs and Users or indeed Users assigned subordinate Users.
- They may also be used to authenticate SAMs and Users to the Platform.
- The Platform grants to the User one or more privileges that may be associated with one or more SAMs, or resources controlled by a SAM but directed via an external Privilege Provider.
    - The privileges may be time limited (requiring renewal).
    - The privileges associated with a User may change over time or be dictated in real time by the external Privilege Provider
    - The App manages a User's credential and privileges, making them available to the SAM or Platform depending on the context. A User may also directly manage credentials via the platform utilizing any other suitable device or system, including the functions and capabilities of the asset itself directly via the Platform.
    - The App or any other device of privilege assertion must protect the confidentiality, integrity and availability of the credential and privileges.

[0040] This design supports high levels of scalability and considerable flexibility in the way that the system is deployed, thus supporting the aim of a reusable architecture that supports a range of disparate applications.

Overall Security Requirements

[0041] In any distributed system there are risks associated with the potential for introducing forged credentials into the system to support a masquerade at-

tack. Similarly, the storage of privileges under the control of the User implies that these could be forged or modified. The key security requirements therefore focus on these two risks:

- Credentials to identify a User/SAM must be protected from forgery. Credentials to identify a User/SAM must be protected from modification.
- Credentials to identify a User/SAM must be protected from unauthorised deletion/removal. Privileges granted to Users must be protected from forgery
- Privileges granted to Users must be protected from modification.
- Privileges granted to Users must be protected from unauthorised deletion/removal.

[0042] In addition, as the source of all trust in the system, the Platform must be protected from attack; attacks could be against the credential and privilege issuing services, or against the platform itself to prevent it from providing its services.

[0043] The App function is intended to operate on any capable mobile device, such as a smart phone or tablet computer, token of privilege assertion or within the sensor capabilities of the Asset itself. These devices are outside the control of the system and could be suborned to either attack the App directly (e.g., by attempting to attack the User Credentials or privileges under the control of the App), or by using the App as a vector to attack a SAM or the Platform. The App must be protected from attacks on its confidentiality, integrity and availability. The degree of reliance placed on the underlying platform by the App must be minimised to protect the confidentiality, integrity and availability of interactions between the User and the App. Communication between the App and the SAM must be protected against attacks on the confidentiality and integrity of the communications channel and its content. Communication between the App and the Platform must be protected against attacks on the confidentiality and integrity of the communications channel and its content.

[0044] The SAM (and by extension the resources it manages) must be protected from attacks. These may come from the environment in which it is located (e.g., a SAM in a vehicle must be protected from CANBUS attacks as well as attacks on its physical form) or from the external communications channel or technology to the App or Platform. The SAM must be protected from attacks on its confidentiality, integrity and availability that derive from its external communications and from attacks that derive from its environment.

Cryptography

[0045] Cryptography will be used to meet many of the security requirements. Symmetric cryptography could be used to implement an access control framework suitable for distributed systems, for example Kerberos V is an implementation of an underlying mechanism defined by Needham and Schroeder that is widely used (e.g., it is the basis of the Microsoft Windows network security protocols). However, Kerberos requires a relatively tight coupling between the Users, Services and the Ticket Granting and Key Distribution servers; it requires a central repository of symmetric keys that will not scale well. If a centralised privilege key repository is to be avoided, then one approach would be to distribute the keys to the participants once they have been 'registered' – however, this contradicts one of the design principles ("The SAM does not require pre-knowledge of the identity of users or their privileges") as the SAM would have to have knowledge of this information for each User.

[0046] Asymmetric (public key) cryptography supports a loosely-coupled model that scales well. Although a central service is required to distribute public keys, the use of X.509 public key certificates (PKC) removes/reduces the reliance on the central service (a Certification Authority – CA) once the X.509 certificates have been issued to the participants. Ephemeral trust relationships can be created between participants by exchange of X.509 certificates (and proving control of private keys) without reference to the CA – however, it should be noted that the CA may be a source of revocation information and therefore it may not be completely de-coupled.

[0047] It is possible to incorporate a variety of information within an X.509 certificate, although this is largely related to the identity of the certificate owner (Subject), the CA (Issuer) or constraints on the usage of the certificate. It would be possible to place privileges associated with the certificate Subject into the certificate, however, the use of an X.509 attribute certificate (AC) is more appropriate and this is the basis of the design.

[0048] The relationship between a PKC and AC is often compared to that of a passport and a visa; a passport is a relatively long-lived statement of identity, whereas a visa is a relatively short-lived permission to enter a specific country for a fixed period of time and is normally issued by a different authority than the passport. A person may have a single passport containing many visas, all or some of which may be valid concurrently.

[0049] For this system it is proposed that a PKC be used to represent the user's identity and ACs be used to convey privilege information (Capabilities in the terminology of the Capability-Based model).

[0050] Generally, the issuance and management of X.509 PKCs is performed by a Public Key Infrastructure (PKI), whilst the equivalent function for X.509 ACs is performed by a Privilege Management Infrastructure (PMI). PKI and PMI may be separate systems, or combined – this provides considerable flexibility for the implementation, allowing the privilege management functions to be devolved to an appropriate Attribute Authority (AA).

Security Requirements

[0051] The use of public key cryptography introduces a number of security requirements that are specific to the technology (these are neither less, nor more onerous than those imposed by a symmetric cryptographic system –just different).

[0052] Whilst an underlying concept of asymmetric cryptography is that public keys may be widely distributed, the private keys associated with those public keys must be closely guarded.

[0053] Asymmetric algorithms are designed such that knowledge of a public key does not allow the associated private key to be determined; the binding of a public key to a particular identity is the basis of any authentication scheme using the technology. The creation of that binding and its protection against modification attacks is critical; similarly, guarding against the creation of fraudulent bindings:

- All private keys must be protected against attacks on their confidentiality, integrity and availability.
- All asymmetric key-pairs must be generated in a manner that protects the confidentiality and integrity of the operation (including artefacts of the operation).
- All random numbers used in the creation of asymmetric key-pairs must be created with sufficient entropy to guard against guessing attacks.

[0054] A Subject's identity and possession of a private key must be established with certainty prior to binding the identity and associated public key within an X.509 public key certificate.

[0055] Authentication schemes based on X.509 PKC and asymmetric cryptography are reliant on trust in the CA that issued the PKC – this is termed the Trust Anchor (TA) and consists of the public key of the CA (or superior CA in a hierarchy). Typical attacks aim to substitute the TA with a forgery.

[0056] Distribution of TA values must be conducted in a manner that protects the TA value from attacks on its integrity and availability.

[0057] Distribution of TA values must be conducted in a manner that guards against substitution of the values.

[0058] Attribute certificates are nominally the same as public key certificates – they are both signed objects containing information – the difference is in the content. The major risks associated with AC are that they could be modified; they could be fraudulently bound to an incorrect PKC:

[0059] Ownership of a public key certificate must be established before incorporating a reference to that certificate in any attribute certificate.

Network Security Protocols

[0060] The system relies heavily on networked communications between the components. It may be assumed that the underlying networks are not trusted and that the communication between the components can be attacked from the network. The design relies on the use of Transport Layer Security (TLS) to protect communications across untrusted networks.

[0061] It is likely that the system will be implemented across wireless network paths – using technologies such as cellular and wireless data (GSM/GPRS/3G/4G/5G and onwards), WiFi (802.11x), Bluetooth, UWB, Zigbee, Ethernet. Where possible the security features of these technologies should be employed to reduce the attack surface of the system components. Such technologies may also evolve to become the bearer for CanBus or future technologies such as FlexRay and as such, the capability will be to segregate and secure data and data flows from this system from latent data within the asset.

Security Requirements

[0062] Any network protocol may be subject to three common attacks: Eavesdropping allows the confidentiality of the information to be compromised; masquerade allows an attacker to substitute his own identity for that of the trusted party; modification allows an attacker to substitute valid data for invalid data:

- Data transferred across any communications channel must only be accessible to the entities at either end of the channel.
- The identity of the entity at either end of the communications channel must be established prior to transferring any data through the channel.

- The origin of any data received from the channel must be verified to ensure it came from the corresponding entity and has not been modified.

[0063] The assumption is that TLS will protect communications between components, however, the underlying security features of the networking technology employed should be used e.g., SSAM hiding. Security features of the networking technologies used to allow communications between the system components should be enabled and configured to minimise the threat to confidentiality, integrity and availability.

[0064] Referring now to Figures 7-10, the sample application selected is a vehicle security system. In essence it allows a vehicle user to access common vehicle security-related futures, such as locking/unlocking doors and starting/stopping the engine, using a smart phone application or capabilities to assert an identity relating to privileges itself via biometric capabilities or alpha numeric input capabilities.

[0065] The SAM will be embedded in the vehicle – either as a discrete module, or as a chipset resident within a host module. The SAM will interact with the Platform via a cellular data connection; interaction with the App will utilise Bluetooth but could feasibly be any short range wireless data bearer technology.

[0066] The App will be resident on a smart phone using any of the popular mobile operating systems (e.g., iOS, Android, Windows Mobile) or the App function could be incorporated into the operating system of the asset. The App will incorporate all of the cryptographic functionality that is required for it to operate (to remove dependence on the host operating system) and will include a number of security features (see below).

[0067] Implementation of the Platform offers a number of options. Given the intention of using relatively standard PKI and PMI functions, it is straightforward to:

- Create a hierarchy of CAs – for example a root CA (controlled by the system manufacturer), with subordinate CAs controlled by each vehicle manufacturer.

- Create a network of AAs. In general, truly hierarchical PMIs are discouraged (RFC5755 1.2) however this does not preclude the creation of multiple AAs, one of which could be controlled by the vehicle manufacturer, another by a leasing or car rental company.

[0068] On this basis the Platform represents a logical entity that could have its functions distributed amongst multiple, potentially unrelated, participants. For the purposes of this discussion the Platform will be treated as a single physical entity4. The Platform acts as a CA and AA and incorporates the necessary technology to implement these functions, including database technology to store information about SAMs, Users and their privileges. The critical nature of the Platform as the basis of all trust requires that the public keys of the CA and AA are generated, stored and operated within a Hardware Security Module (HSM), with appropriate technical and procedural controls to protect its operation.

Functions and Processes

SAM Registration

[0069] It is visualised that this activity will take place during the manufacturing lifecycle of the asset, either at the point where the SAM is integrated with the vehicle or during the manufacture of the SAM as a component.

[0070] Registration involves the generation of a key-pair within the SAM cryptographic module; the creation of a signed certificate request and its submission to the CA. The SAM must be assigned a unique name (the Subject of the certificate), but it is also possible to incorporate other unique identifiers. In the vehicular context, this would commonly be the "VIN", Vehicle Identity Number, but also could comprise the Engine number, Chassis number etc.

[0071] This depends upon the point in the manufacturing lifecycle at which registration is performed – on balance it is probably preferable to do this during vehicle integration, as it allows the association between a SAM and a vehicle to be crypto- graphically bound (otherwise the SAM-VIN association only exists in the Platform database).

[0072] Communication between the SAM and the Platform will employ the Enrolment over Secure Transport (EST) protocol (RFC7030)5 using an explicit TA that must be distributed within the SAM firmware. As the SAM does not include a user interface, and the initial enrolment is a secure activity, the SAM must be operated in a controlled and secure environment until this action is completed.

[0073] Note that a further use case – SAM Re-Enrolment – deals with renewal of SAM identity credentials. This use case has not been developed, but in principle uses EST and the current SAM credential to automatically renew the credential before its expiry. There are further boundary use cases to deal with, for example, renewal of expired or revoked credentials.

[0074] On completion of registration the SAM will have:

- An asymmetric key-pair.
- A PKC containing the public key and binding to the SAM unique identity (and potentially the vehicle unique ID).
- A 'registration' in the Platform that can be used to target privileges or accept privilege containers from external privilege providers.

SAM Policy

[0075] The SAM must be able to autonomously make decisions based on its environment or context. The concept of a Policy is that it is a set of rules that aids the SAM decision making. The policy could include rules such as:

- How to handle extended loss of communication with the cellular network (e.g., this means that no revocation information can be received from the Platform).
- How to respond when a Privilege to operate the vehicle ends (e.g., lock the vehicle next time the User exits, enter 'limp' mode for the engine management unit).
- Utilise any contextual elements (e.g., time, location, privilege being requested by specific Identified User) in order to derive a percentage likelihood of a legitimate assertion of privilege and au-

thenticity of User upon which a threshold can be set to either grant that privilege or grant a benefit of doubt privilege that can be dynamically affirmed or rescinded at a point when, for example, full communication access to the platform is re-established and benefit of doubt granted privilege can be affirmed, rescinded or modified.

[0076] A default policy should be installed in the vehicle during manufacture (this is a secure activity, similar in some ways to the SAM registration). Subsequently, a system-level privilege is the ability to change some or all policies.

Privileges

[0077] The term Privilege represents a set of privileges associated with a user; they will normally be contained within an attribute certificate but may only exist within the Platform database or as entries within an external Privilege Providers database until the user requests the attribute certificate. In some cases, an attribute certificate is not required – e.g., interactions with the Platform to create new Privileges (as the Platform knows the Privileges associated with a user).

[0078] Typical privileges associated with a vehicle include:

- Locking/unlocking vehicle doors, bonnet, boot, fuel cap, charging port
- Starting/stopping the engine
- Vehicle performance capabilities
- Access to in vehicle service typically contained and represented within the In Vehicle Infotainment system such as external cameras, navigation and telematics, vehicle diagnostics, off-board content and entertainment
- Hardware dependent functions such as intelligent cruise control, services derived from sensors, climate control, anthropomorphic adjustments etc.

[0079] In addition there are 'system' level privileges:

- Create a new Privilege that assigns privileges to a new User

- E.g., Permit somebody else to operate the vehicle or permit somebody to conditionally operate or interact with a vehicle
- Transfer ownership of the vehicle
- Revoke or assign the privileges of a User or subordinate User
- Change the SAM Policy

[0080] When the vehicle is first manufactured, the manufacturer has a 'full' Privilege. In order to transfer control over the vehicle to a Dealer, the manufacturer must grant Privileges to the Dealer.

[0081] A Privilege is associated with a single SAM – the SAM identity is included in the attribute certificate. In addition, other security-related information may also be included in the AC – for example, a Bluetooth MAC address.

Dealer

[0082] A Dealer is an intermediary between the vehicle manufacturer and the end customer (User). The Dealer (like the vehicle manufacturer) must receive credentials from the Platform – but it is unlikely that these will be used via a mobile app. The use of a smart card or similar cryptographic token to protect the Dealer credentials is recommended.

[0083] The Dealer interacts with the User to register the User with the Platform as well as granting a Privilege to the User for a vehicle – as part of the delivery process for example.

Third Parties

[0084] A Third Party in this context is somebody with control over the vehicle, typically because they own it (e.g., a finance company, car rental company, etc.). They have the right to grant a Privilege to a User (who is actually going to operate it), but retain control over that Privilege (so it could be revoked if, for example, payments on a finance agreement are not made).

User

[0085] In this system, a User is someone with control over a vehicle who holds the prerequisite privilege and has asserted his identity to enact those privileges to which he has access. A User may be the legal owner of the vehi-

cle, or a 'temporary' user. For example, a vehicle provided under a finance agreement will legally belong to the finance company, in which case the User is a temporary user until the finance agreement ends. In this case it is unlikely that the User would receive the 'Transfer ownership of the vehicle' privilege. The duration of a User's access to the vehicle is determined by the validity period of the attribute certificate containing the Privilege.

[0086] A User may grant privileges to other Users, but this is constrained by their own Privilege. A User may grant any privilege that they have, or any subset of privilege that they see fit but is contained within their privilege rights as defined by their title to the asset or that offered by the Privilege Provider of the specific privilege function.

User Registration

[0087] Registration of a User is conducted within the App, which is responsible for creating the key-pair and requesting a PKC from the CA. This could also employ the EST protocol described above, but with some variations. The identity of the User must be verified before the PKC can be issued – this should be undertaken by a trusted party; for the purposes of this discussion it is assumed that this will be the Dealer (but could equally be a finance company, car rental company, etc.).

[0088] In PKI terms, the Dealer is acting as a Registration Authority (RA) and provides temporary credentials (a one-time password and serial number) to the User for use in the registration process. These temporary credentials are sufficient to authenticate the User prior to issuing the PKC – the Dealer may capture a range of information about the user for presentation to the Platform (name, email address, mobile phone number, etc.).

[0089] On completion of the registration process, the User (App) will have:

- An asymmetric key-pair.
- A PKC containing the public key and binding to the User unique identity.

- A 'registration' in the Platform that can be used to target privileges.

[0090] As the key-pair is specific to a single App instance, and the User may possess multiple mobile devices, or lose a mobile device, there are a number of use cases around managing this variation. For example, a registered User could 'vouch for' his identity on another App instance. A User is likely to have multiple PKCs associated with his identity.

User Privilege Assignment

[0091] It should be noted that the creation of a User identity (a PKC) is independent of the grant of a Privilege (AC) – they may be combined into a single business process. Any of the actors with Privilege for a particular vehicle may grant a Privilege to a User. For the simple use case, it is assumed that this is done by a Dealer:

- The Dealer authenticates to the Platform (TLS with mutual authentication)
- The Dealer specifies the User, the SAM and the Privilege to grant (the Platform verifies that the Dealer has the Privilege to do this)
- The User, via the App, authenticates to the Platform (TLS with mutual authentication) and downloads any pending Privilege(s)

[0092] If the User should decide to grant a Privilege to another user the same process is used:

- The User, via the App, authenticates to the Platform (TLS with mutual authentication)
- The User specifies the new User, the SAM and the Privilege to grant (the Platform verifies that the User has the Privilege to do this)
- The new User, via their App, authenticates to the Platform (TLS with mutual authentication) and downloads any pending Privilege(s)

[0093] The other use cases discussed, e.g. finance company, car rental company, etc. would interact with the system in an identical manner.

Privilege Revocation

[0094] A mechanism for revoking Privileges is required – although revocation information may be of interest to a User, it is primarily for use by the SAM.

[0095] There are some constraints that influence a revocation mechanism:

- The SAM may not be connected to a cellular data service at all times
  - An 'on-line' check of revocation status (e.g. using OCSP or similar mechanism) is potentially expensive, and may not be feasible (if not connected to a data service)
  - A 'push' mechanism may not be feasible, if the SAM is not connected to a data service
- The SAM has a finite storage capacity for storing revocation data
  - Probably not an issue for the general use case
  - Certainly an issue for some use cases, e.g. hire cars, pool cars, etc.

[0096] The recommended approach is to use SMS messages to push revocation information to the SAM on demand (i.e. following a revocation). The use of SMS is suggested because it represents the lowest common denominator for cellular data transfer – in particular it works with a basic 2G/GSM service and does not require access to a data service. The SMS revocation message will consist of an identifier for the revoked AC, an expiry date for the revocation8 and a digital signature. The primary purpose of the expiry date is to allow 'garbage collection' by the SAM, to ensure that storage resources are managed; the signature protects against DOS attacks.

[0097] Other methods are also applicable but not contained within this example such as the Open Mobile Alliance Light Weight M2M messaging protocol.

[0098] The Platform will implement an assured delivery mechanism – once a revocation message has been created, the Platform will continue to resend the message until an acknowledgement has been received.

[0099] It may be possible to extend this mechanism to the App, but it is probably more efficient for the App to 'collect' revocation data when it is next

connected to the Platform. This could be done as an extension to the Privilege granting mechanism – e.g. a request for pending privileges results in the removal of expired and revoked privileges, as well as downloading new ones.

[00100] Note that this is one area where SAM Policy is required to manage boundary cases (or a potential attack on the SAM). For example, the Policy rules could determine how the SAM processes a Privilege if it is not connected to a cellular network, or has not been so for an extended period.

Use Cases

[00101] The primary use cases are focused on the core functionality of the system: The vehicle is manufactured; it is transferred to a Dealer; the Dealer sells the vehicle to a User; the User uses the vehicle.

[00102] The Vehicle Manufacturer carries out the following steps, illustrated in Figure 7:

- Integrate SAM with the vehicle and create an association between SAM and the Vehicle Identification Number (VIN);
- Register SAM with the Platform and receive PKCs from CA;
- Install default policy;
- Receive full privileges for the vehicle.

[00103] Figure 8 illustrates the transfer of the vehicle to the dealer. The Vehicle Manufacturer creates a Privilege set for the Dealer in respect of the vehicle. This transfers to the SAM full privileges. The Dealer downloads the Privilege set for the vehicle SAM and sets a market-specific policy.

[00104] Figure 9 illustrates the transfer of the vehicle from the dealer to the User. The Dealer initiates registration of the User and transfers the registration credential (Serial Number/OTP) to the User. The User completes registration with the Platform and downloads and installs the PKCs. The Dealer creates the Privilege set for the User, and the User downloads this from the Platform.

[00105] Figure 10 illustrates the granting of User access to the vehicle. The User connects his mobile phone, for example, to SAM via Bluetooth. The devices mutually authenticate via TLS. The Privilege set is supplied to the SAM,

and then the User makes an access request. The SAM validates the privilege, granting or denying the access request according to the Privilege received.

Security Considerations

App Security

[00106] The App must operate in a context where there is no trust in the underlying operating system, or any inputs that are dependent upon the operating system. Note that in a more highly controlled environment, it may be possible to gain some trust in the underlying platform services offered by the operating system, but in this context it is not practicable.

[00107] The App must protect the User credentials (private key, PKCS, Privileges) on behalf of the User. It is important, therefore, that interaction between the User and the App is preceded by robust authentication of the person claiming to be the User. It is strongly recommended that a multi-factor approach is adopted, using a combination of:

- PIN or passphrase
- Simple biometrics (e.g. facial geometry, pattern selection, pattern creation)
- Complex biometrics (e.g. fingerprint, iris, face)

[00108] Note that the lack of trust in the underlying platform must also extend to the sensors and other devices used to provide input. Although a multi-factor approach could be defeated by a sufficiently capable attacker, it is a potentially difficult target.

[00109] For similar reasons, it is essential that the cryptographic functions and security protocols (TLS) are an embedded part of the App, to avoid having to trust platform services. It is suggested that digital signatures are used to verify the integrity of the App components whenever its starts up.

SAM Security

[00110] As an embedded device, the SAM has less surface to attack compared to the App. However, a self-contained firmware environment that in-

cludes all cryptographic functions and is digitally signed will reduce the risk of attack.

Off-line Mode

[00111] In some uses of the technology, continuous communication between the authenticator and the access device may not be possible. For example, where the access device is associated with a movable set of resources such as a motor vehicle, the user may wish to exercise the privileges at a location where radio-based communication is not possible – an underground parking garage, say. In such circumstances, provision needs to be made for the granting of interim access pending re-establishment of communication between the access device and the authenticator. It is envisaged that the vehicle could be provided with an externally-accessible interface by which the user can establish identity to the access device if a separate token or key, or a smart phone is not used. The access device can then use pre-stored data, downloaded when communication was possible between the authenticator and the access device, to determine whether interim exercise of privileges should be granted. Thus, in the case of a hire car, the initial identity data might be transmitted to the car on making of the booking, or as soon afterwards as communication with the car is possible, to be stored in a secure cache in the access device until the user wishes to commence use of the car. When communication is subsequently re-established, the access device may then request the user to confirm identity, for example within a predetermined time, as a condition for continued grant exercise of the privileges, or as a condition for exercise of the full range of privileges as opposed to a limited sub-set of privileges.

Glossary / Terms

[00112] Asset – A physical or non-physical entity which provides service, function or value to a person or entity with appropriate ownership or privilege to access or facilitate such from the asset or contained within.

ID Control Module (SAM) - is a Secure Access Module being either hardware module, ASIC or software to enable the security, communication and privilege management functions of the system.

Privilege – A right to use, access or modify a function contained within or presented via an Asset

Privilege Capabilities – A roster of specific functions or capabilities available within an Asset to which privilege can be appended.

Privilege Provider – An external function for the procurement and deliver of specific service or functions available within the roster of Privilege capabilities within an Asset.

CLAIMS

1. An access authorisation system, comprising a central authenticator and an access device controlling access to each of a plurality of resources, the access device being remote from the central authenticator and being programmable and configured to communicate therewith, wherein the authenticator stores:

for each of a plurality of users, a user identifier and user identity data associated therewith;

for each of a plurality of access devices, an access device identifier and data relating to each of the resources controlled by the access device; and

at least one privilege granted to each user to use at least a selected one of the plurality of resources controlled by at least one of the access devices;

wherein the authenticator and the access device are programmed to perform the following steps in response to the user requesting from the authenticator exercise of the privilege:

(a) in response to receipt of the request, the authenticator requests the user to provide to the authenticator individual identifying data for the user;

(b) the authenticator compares the sent data with stored data to verify the user's identity;

(c) the authenticator transmits to the access device instructions to allow the user to exercise the or each privilege.

2. An access authorisation system according to Claim 1, wherein the user is a person and the authenticator is programmed in step (a) to request the user to provide personal identifying data.

3. An access authorisation system according to Claim 2, wherein the personal identifying data comprises one or more of a personal identification number and unique physical characteristics of the user.

4. An access authorisation system according to Claim 3, wherein the unique physical characteristics are a fingerprint, a retina pattern, a face image or part thereof, and a speech sample.

5. An access authorisation system according to Claim 2, 3 or 4, further comprising a user device remote from the central authenticator and programmable and configured to communicate with the access device and with the central authenticator, wherein the user device, the authenticator and the access device are programmed to perform the following steps in response to the user causing the user device to request from the authenticator exercise of the privilege:

(a1) in response to receipt of the request, the authenticator instructs the user device to display to the user a request to input personal identity data;

(a2) the user device transmits the personal identity data input by the user to the authenticator and the authenticator compares this with stored data to verify the user's identity;

(a3) the authenticator transmits a transaction token to the access device and to the user device;

(a4) the user device communicates with the access device to request exercise of the privilege, the communication including the user device transaction token; and

(a5) a matching operation is performed on the user device transaction token and the access device transaction token and the access device is arranged to allow exercise of the or each privilege if the result of the matching process meets predetermined criteria.

6. An access authorisation system according to Claim 5, wherein the matching operation is performed by the access device and comprises comparison of identical tokens.

7. An access authorisation system according to Claim 6, wherein the access device token and the user device token are two parts of a master token generated by the authenticator, and the matching operation comprises the access device combining the access device and user device tokens and transmit-

ting the combined token to the authenticator, and the authenticator comparing the combined token with the master token and transmitting an authorisation to the access device if the agreement between the combined token and the master token is within predetermined criteria.

8. An access authorisation system according to Claim 5, 6 or 7, comprising encrypting the tokens before transmission.

9. An access authorisation system according to any preceding claim, wherein the authenticator is further programmed to request identifying data from the access device and/or from a resource connected thereto before performing step (c).

10. An access authorisation system according to Claim 9, wherein the identifying data comprises location data.

11. An access authorisation system according to any preceding claim, wherein the resources to which the access device controls access are configured as at least one primary resource and at least one secondary resource accessible only when access has been granted to the respective primary resource.

12. An access authorisation system according to Claim 11, wherein the access device is programmed to provide continued access to the or each secondary resource only if one or more additional criteria are fulfilled.

13. An access authorisation system according to Claim 12, wherein the additional criteria are selected from: current date or time; proximity of the user; status of the resource; geo-spatial co-ordinates; pattern of operation; connectivity; consumption; and association with other resources.

14. An access authorisation system according to any of Claims 11 to 13, wherein the access device is programmed to receive preliminary user and privilege data from the authenticator and to store this for subsequent use in allowing provisional access to a resource when communication between the access device and the authenticator is interrupted, the access device being further programmed to seek confirmation of identity from the use when communication with the authenticator is re-established before allowing continued access or allowing full access to all resources for which privileges have been granted.

15. A secure data communications system, comprising first and second programmable devices configured to communicate with each other and with a remote server device configured to issue at intervals to the first device and the second device an encrypted security code, the system further being configured such that, when any of the devices initiates communication with any of the other devices by transmission of its security code, the receiving device compares the received code with the most recent security code received from the server and only allows communication to continue if the conformity between the codes and their transmission criteria is within predetermined limits.

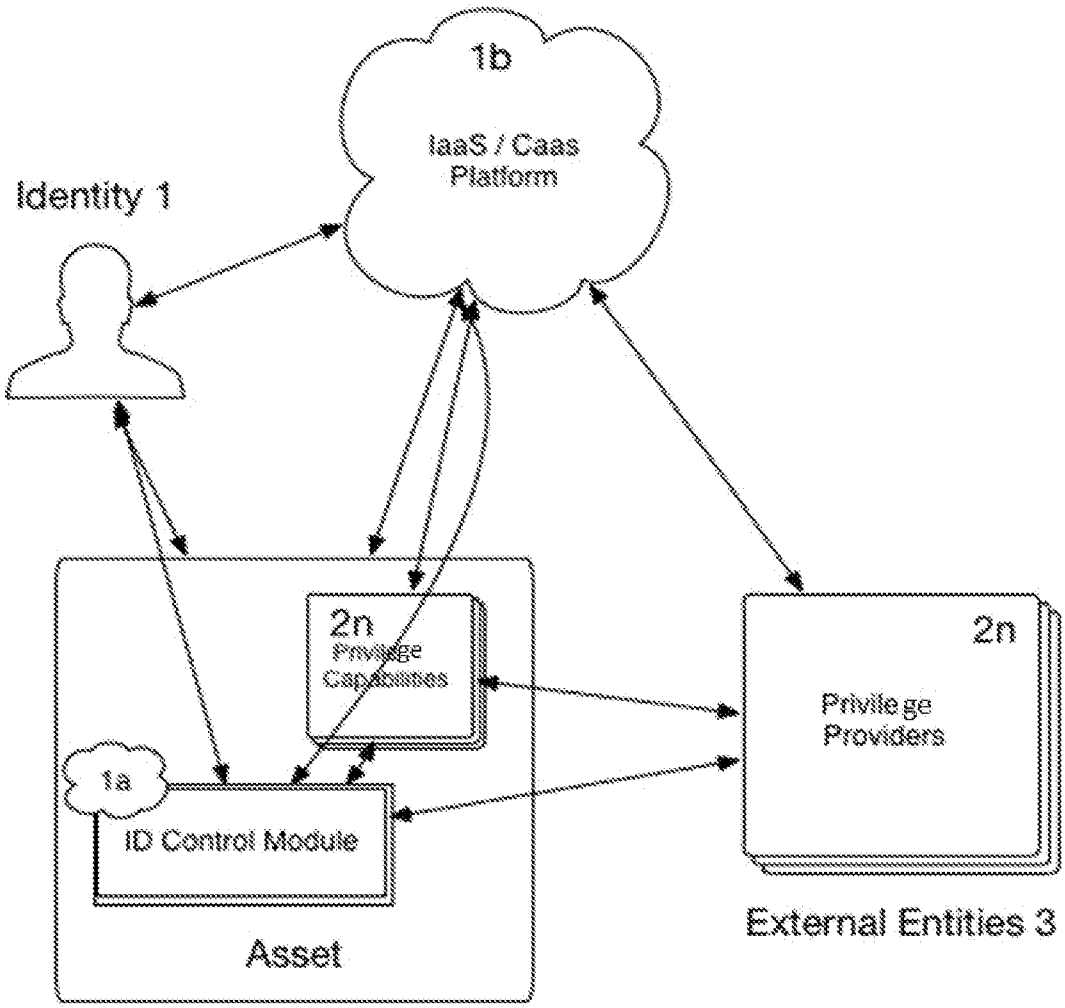

1b
IaaS / Caas
Platform
Identity 1
2n
Privilege
Capabilities
1a
ID Control Module
Asset
2n
Privilege
Providers
External Entities 3

Fig 1

Fig 2

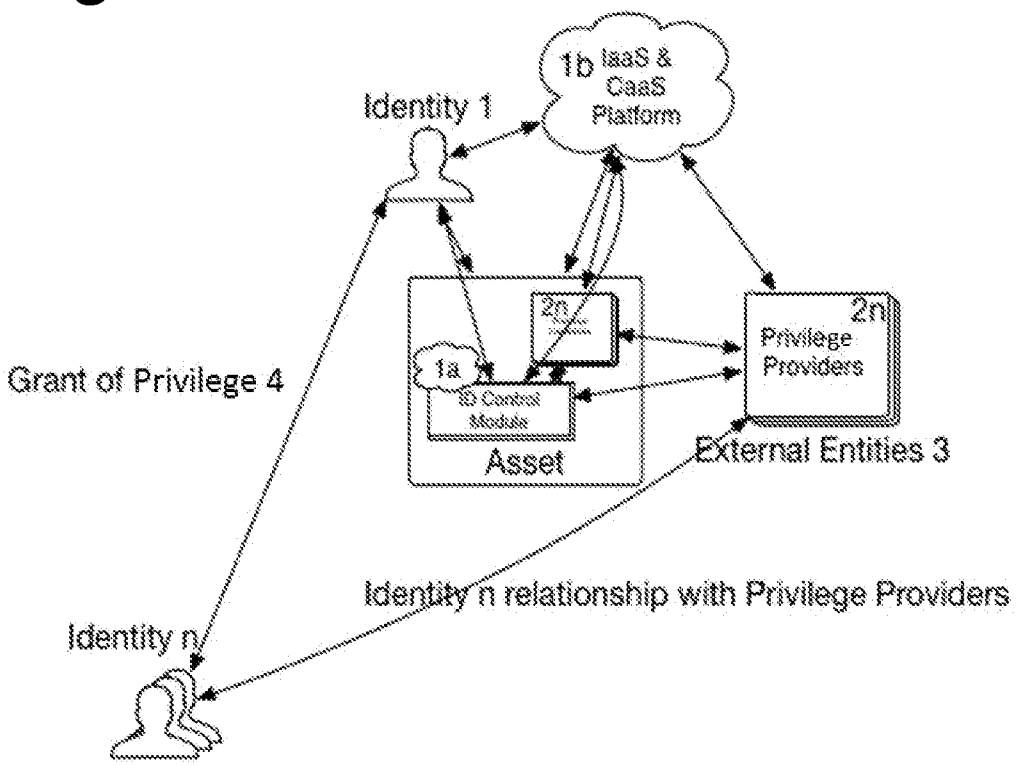

1b IaaS & CaaS Platform
Identity 1
2n
1a
ID Control Module
Asset
2n
Privilege Providers
External Entities 3
Grant of Privilege 4
Identity n relationship with Privilege Providers
Identity n

Fig 3

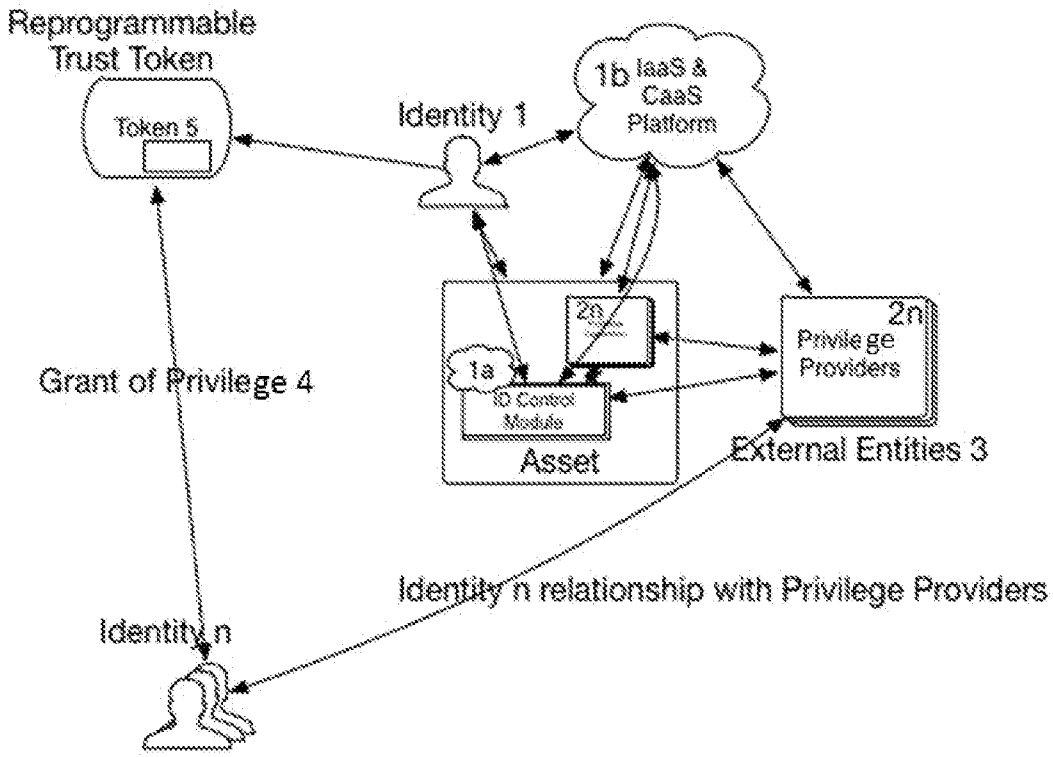

Reprogrammable
Trust Token
Token 5
Identity 1
1b IaaS &
CaaS
Platform
2n
Privilege
Providers
2n
1a
ID Control
Module
Asset
Grant of Privilege 4
External Entities 3
Identity n relationship with Privilege Providers
Identity n

Fig 4

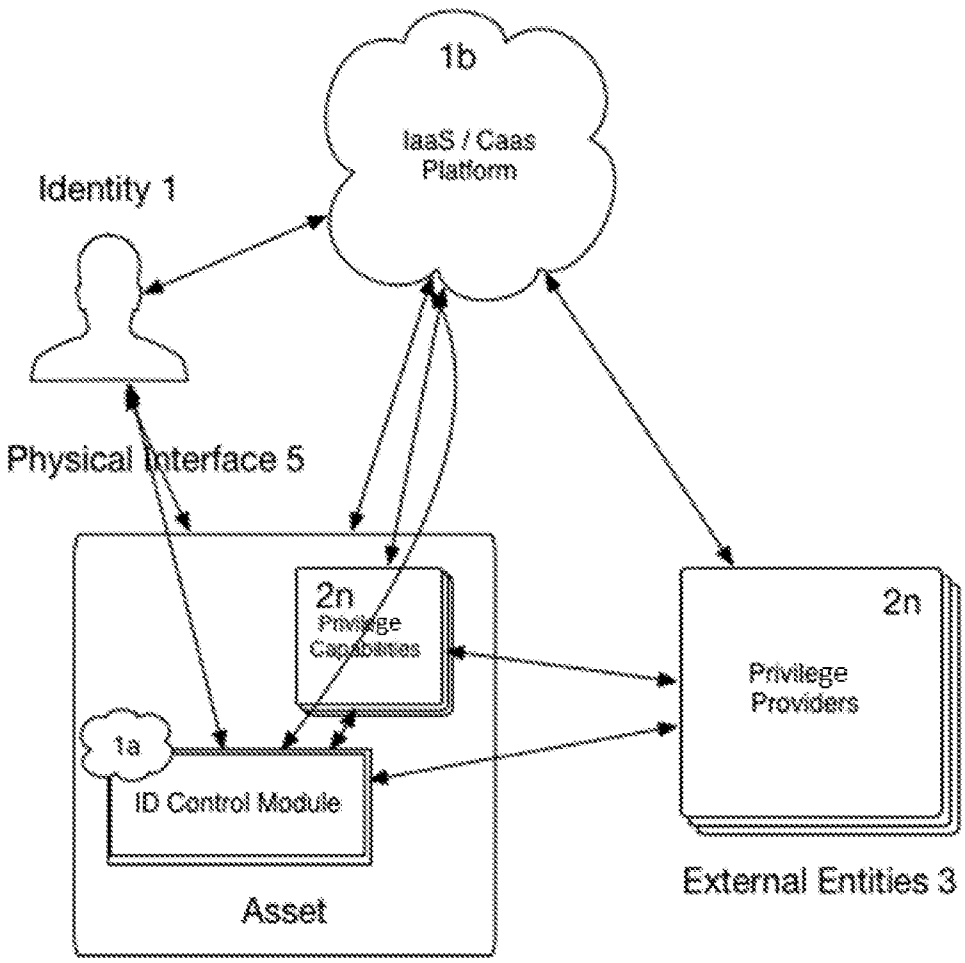

1b
IaaS / Caas
Platform
Identity 1
Physical Interface 5
2n
Privilege
Capabilities
1a
ID Control Module
Asset
2n
Privilege
Providers
External Entities 3

Fig 5

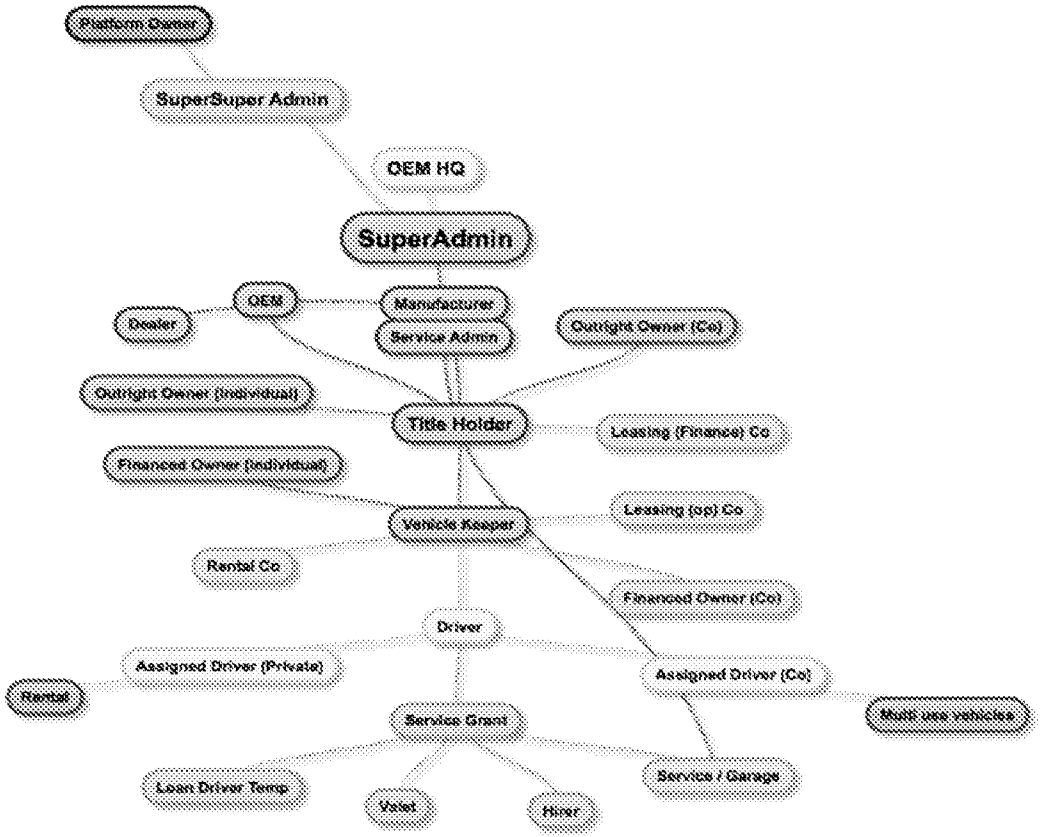
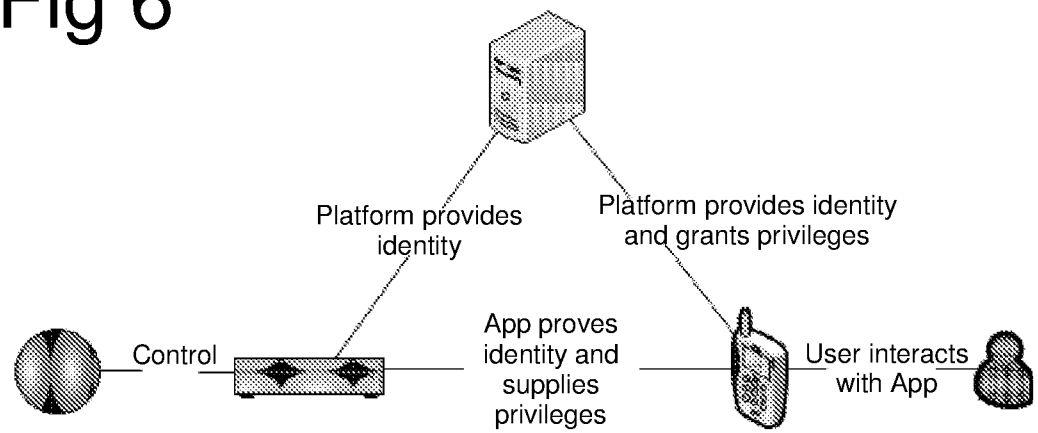

Platform Owner
SuperSuper Admin
OEM HQ
SuperAdmin
OEM
Manufacturer
Dealer
Service Admin
Outright Owner (Co)
Outright Owner (Individual)
Title Holder
Leasing (Finance) Co
Financed Owner (Individual)
Vehicle Keeper
Leasing (op) Co
Rental Co
Financed Owner (Co)
Driver
Assigned Driver (Private)
Assigned Driver (Co)
Rental
Multi use vehicles
Service Grant
Service / Garage
Loan Driver Temp
Valet
Hirer

Fig 6


Platform provides identity
Platform provides identity and grants privileges
Control
App proves identity and supplies privileges
User interacts with App

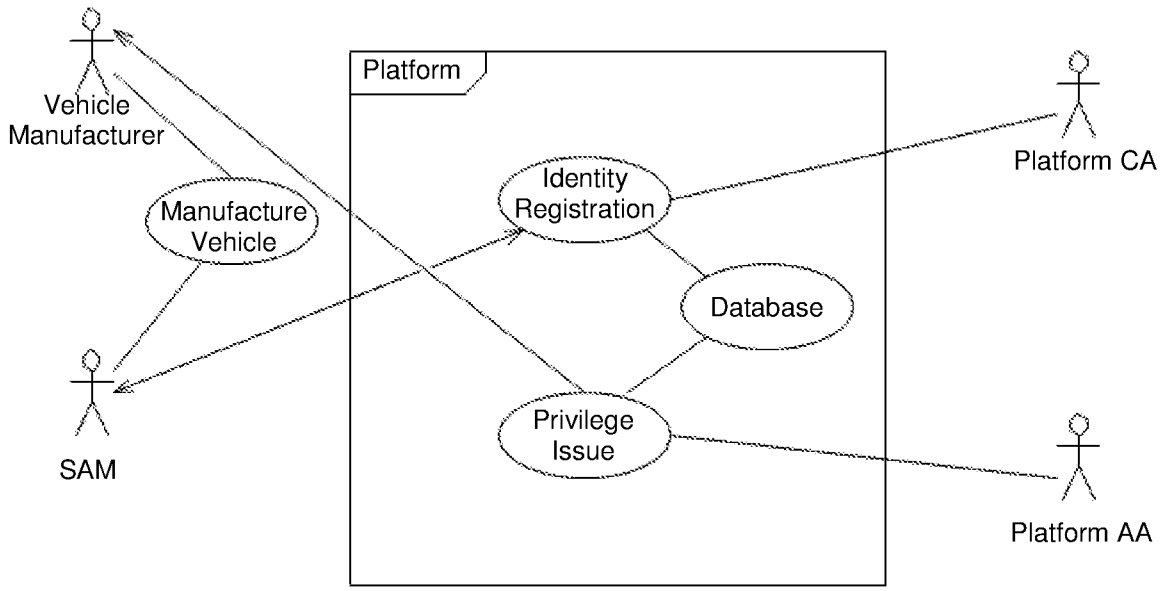

Vehicle Manufacturer
Platform
Platform CA
Identity Registration
Manufacture Vehicle
Database
SAM
Privilege Issue
Platform AA

Fig 7

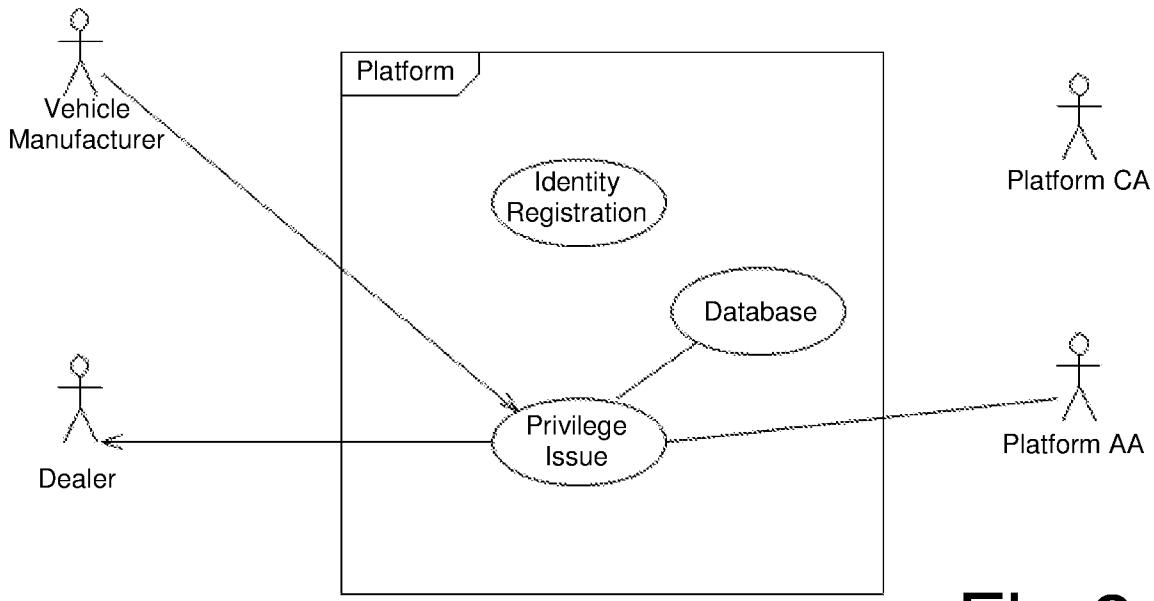

Vehicle Manufacturer
Platform
Platform CA
Identity Registration
Database
Dealer
Privilege Issue
Platform AA

Fig 8

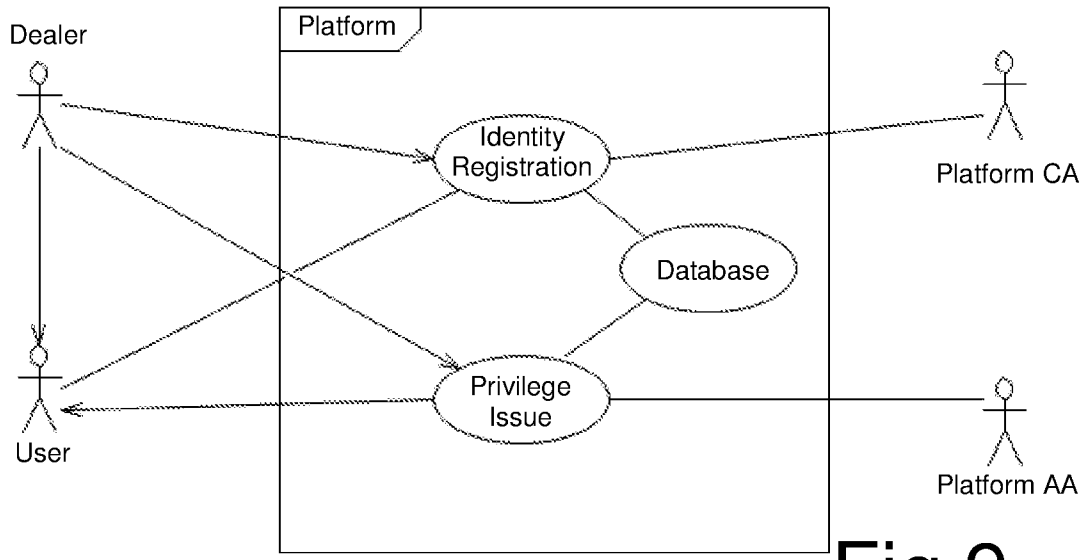

Dealer
Platform
Identity Registration
Database
Privilege Issue
User
Platform CA
Platform AA

Fig 9

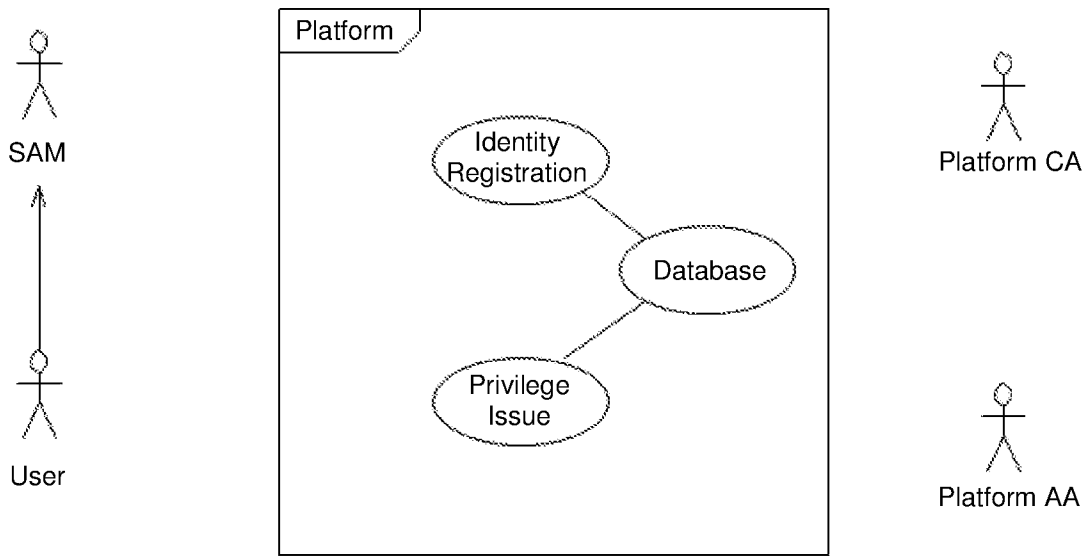

SAM
Platform
Identity Registration
Database
Privilege Issue
User
Platform CA
Platform AA

Fig 10