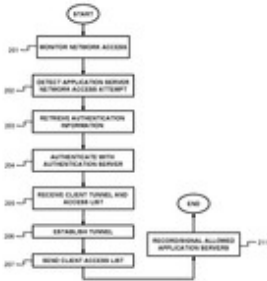
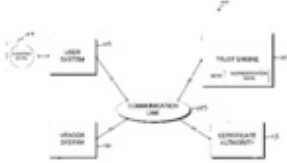


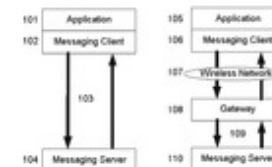
Patent families - 57 results

#	 	Title	Publication number	Publ. date	Applicant/Assignee			
1.		Systems and methods for protecting network devices	EP3205073	2017-08-16		100 %		
Embodiments of the present disclosure help protect network devices from unauthorized access. Among other things, embodiments of the disclosure allow full access to application servers and other network devices that a client is allowed to access, while preventing all access (or even knowledge) of network devices the client is not allowed to access.								
2.		Context sensitive dynamic authentication in a cryptographic system	EP1218813	2002-07-03	 	84 %		
A system for performing authentication of a first user to a second user includes the ability for the first user to submit multiple instances of authentication data which are evaluated and then used to generate an overall level of confidence in the claimed identity of the first user. The individual authentication instances are evaluated based upon: the degree of match between the user provided by the first user during the authentication and the data provided by the first user during his enrollment; the inherent reliability of the authentication technique being used; the circumstances surrounding the generation of the authentication data by the first user; and the circumstances surrounding the generation of the enrollment data by the first user. This confidence level is compared with a required trust level which is based at least in part upon the requirements of the second user, and the authentication result is based upon this comparison.								
3.		Systems and methods for secure transaction management and electronic rights protection	EP1526472	2005-04-27	 	  83 %		
The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, the utilizing the "electronic higher".								

4.	Portable computerized device adapted for ad hoc security associations	US20150143121	2015-05-21	ROUND ROCK RESEARCH ROUND ROCKS RESEARCH	79 %	
A portable computing device configured to provide secure data communications with a network via a network communications interface. In one embodiment, the portable computing device includes a network security apparatus configured to communicate data with other network security apparatus over the network via the establishment of an association, the establishment of the association between the network security apparatus and the other network security apparatus resultant in the execution of a key generation algorithm configured to cause the network security apparatus and the other network security apparatus to exchange information utilized in the generation of cryptographic keys.						
5.	System and method for digital rights management using a standard rendering engine	EP1357456	2003-10-29	CONTENTGUARD	78 %	
A system and method for the secure distribution and consumption of electronic documents using a standard rendering engine. The documents can usage rights associated therewith. A server stores at least one of the documents in computer readable form. A client having a standard application program including a rendering engine capable of rendering unencrypted documents for viewing is operated by a user. The client and the server are coupled by a communications network . A security module controls requested for at least one of the documents on the server from the client and delivers the document and a set of rights associated with the document to the client. <IMAGE>						
6.	Structure of digital rights management (drm) system	EP1259863	2002-11-27	MICROSOFT TECHNOLOGY LICENSING MICRO SOFT TECHNIQUE LICENSE MICROSOFT	77 %	
A digital rights management (DRM) system operates on a computing device when a user requests that a protected piece of digital content be rendered by the computer device in a particular manner. The DRM system has a license store, a license evaluator, and a state store. The license store stores digital licenses on the computing device. The license evaluator determines whether any licenses stored in the license store correspond to the requested digital content and whether any such corresponding licenses are valid, reviews license rules in each such valid license, and determining based on such reviewed license rules whether such license enables the requesting user to render the requested digital content in the manner sought. The state store maintains state information corresponding to each license in the license store, where the state information is created and updated by the license evaluator as necessary.						

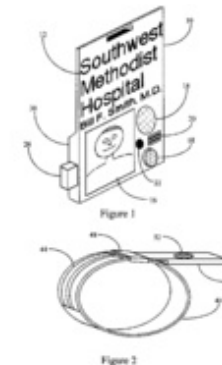
Rank	Topic	WO	Date	Author	Percentage
7.	Systems and methods for providing compensation, rebate, cashback, and reward for using mobile and wearable payment services	WO2017/021882	2017-02-09	ZHOU ANDREW KONAWARE SUNDAY GRID TRAN ZHOU ANDREW HAI BIN 2 more...	77 %

Provided are methods and systems for providing compensation for using a mobile payment service. The method may commence with receiving payment information associated with a user. The method may include generating a unique code encoding the payment information and providing the generated unique code to the user. The method may continue with receiving a deposit amount associated with a purchase related to the user. The purchase may be made via the mobile payment service. The method may further include receiving a notification about a further purchase of the user via the mobile payment service. The notification may include at least the unique code and a product barcode. The product barcode may be associated with the further purchase. The method may further include providing a compensation from the deposit amount to the user. The compensation may be associated with a payment amount associated with the further purchase.



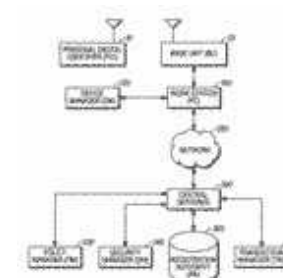
8.	Security badge for automated access control and secure data gathering	US5960085	1999-09-28	DLH TECHNOLOGY	76 %
				SOUTHWEST TECHNOLOGY INNOVATIONS	

A system utilizing a personal identification badge to collect data and to provide access to a computer terminal. The personal identification badge includes circuitry and transceiver components for transmitting identification information and exchanging other **digital** information with a computer terminal and other compatible devices. The personal identification badge establishes a wireless communication link with a computer terminal to allow a user to logon to the terminal. When a user leaves the computer terminal, the communication link is terminated, causing the computer terminal to lock the keyboard, blank the monitor, and/or logoff the user if the communication link is not restored within a sufficient time period. The personal identification badge includes means for encrypting and signing **digital** information. Adapted for use within a hospital, the system provides further means for establishing an affiliation between a personal identification badge and a patient, for collecting **digital** information from electronic devices that record or gather data regarding the status of a patient, for digitizing and recording dictation spoken into the personal identification badge, and for modifying the **digital** information so collected to conform to standards, such as those of a Java applet or the hypertext markup language, for interactive display on a universal display browser.



9.	Method and system for securing a computer network and personal identification device used therein for controlling access to network components	EP1360568	2003-11-12	3M	75 %
		AIT ADVANCED INFORMATION TECHNOLOGIES			

An improved computer **network** security system and method, and a personal identifier device used for controlling **network** access. A new user is registered to a portable personal **digital** identifier device and an input biometric of the user is received and securely maintained in storage. A **private** key is also generated and securely maintained in the storage. When the personal **digital** identifier device is within an envelope area proximate the workstation a first signal is transmitted from a base unit associated with the workstation to the personal **digital** identifier device and the personal **digital** identifier device automatically transmits a response signal establishing communications between the base unit and the personal **digital** identifier device. A digitally and biometrically signed challenge response message is produced and transmitted by the personal **digital** identifier device.



10. Method, device, and system for authentication

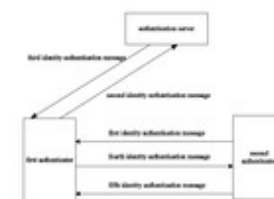
EP2827540

2015-01-21

IWNCOMM

75 %

The present invention relates to the field of identity authentication. Provided are a method, device, and system for authentication, solving the problem that existing identity authentication technologies are incapable of protecting personal privacy, and that authentication technologies comprising personal privacy must provide a traceability feature. The method for identity authentication comprises: a second authenticator transmitting to a first authenticator a first identity authentication message; the first authenticator transmitting to an authentication **server** a second identity authentication message; the authentication **server** verifying the validity of a secure domain where the second authenticator is at and of the first authenticator on the basis of the second identity authentication message; the authentication **server** returning to the first authenticator a third identity authentication message; the first authenticator transmitting to the second authenticator a fourth identity authentication message; the second authenticator proceeding to verification when the fourth identity authentication message is received; the second authenticator transmitting to the first authenticator a fifth identity authentication message; and the first authenticator proceeding when the fifth identity authentication message is received. The authentication system comprises the first authenticator, the second authenticator, the secure domain where the second authenticator is at, and the authentication **server**.



11. Interoperable systems and methods for peer-to-peer service orchestration

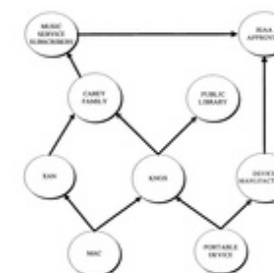
EP2280524

2011-02-02

INTERTRUST TECHNOLOGIES

74 %

A method of managing access to protected content is disclosed, the method being carried out by a content consumption device including a **digital** rights management engine (1000; 1220). The method comprises receiving a request to access a piece of protected content, and using the **digital** rights management engine to evaluate **digital** rights management objects that make up a licence to determine whether permission to access the protected content should be granted, wherein some of the information needed by the **digital** rights management engine to access the content needs to be obtained through external **digital** rights management services. The method further comprises dispatching a service discovery request to locate a node that provides a desired service, and finding candidate service providing nodes, sending a request corresponding to a desired service to a service providing node, receiving a response message from the service providing node, and, if permission to access the protected content is granted, using a media rendering engine to render the content.



12. Platform for computing at the mobile edge

EP3420465

2019-01-02

SMART EDGE COM

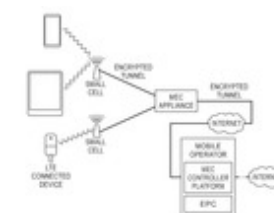
74 %

ACS

ACSS USS

INTEL

Disclosed is a platform for providing computational resources at and/or near a mobile **network** perimeter. The platform may be used to provide computational resources adjacent a small cell radio via at least one Mobile Edge Compute ("MEC") Appliance and at least one MEC Controller. The MEC Appliance can serve as the data plane to support data flow traffic. The MEC Controller can provide a micro-services architecture designed for resiliency, scalability, and extensibility. The platform can be used to decentralize the mobile **network** operator's core **network** and/or associated macro-cell **network** topologies, generating a platform with enhanced flexibility, reliability, and performance. The platform can include a security architecture for effective privacy and access within a distributed topology of the **network** at and/or near the edge of the mobile **network** perimeter.



13. Method for oauth service through blockchain network, and terminal and server using the same

US20190306148

2019-10-03

COINPLUG

74 %

A method for authentication based on a blockchain **network** is provided. The method includes steps of: an authentication-supporting **server** (a) if verification is requested by a certificate authority (CA) app, verifying a **signature** value and transmitting an access token to a user device, supporting the CA-affiliate app to transmit a login request to a CA-affiliate **server**, and registering the access token in the blockchain **network**, and transmitting a verification request to the blockchain **network** to transmit the access token to the authentication-supporting **server**, and register the access token in the blockchain **network**, and transmitting the access token to the user device, and transmit the login request to the CA-affiliate **server**, and (b) performing one of (i) verifying the access token, and (ii) transmitting the verification request to the blockchain **network**, and transmitting a verification-result to the CA-affiliate **server**, to allow the CA-affiliate app to log in to the CA-affiliate **server**.

