United States Patent and Trademark Office

PATENTS

Home | Site Index | Search | FAQ | Glossary | Guides | Contacts | *e*Business | eBiz alerts | News | Help

Patents > Guidance, Tools, and Manuals >> Classification >>> Class Definition

Class Numbers & Titles | Class Numbers Only | USPC Index | International | HELP

You are viewing a Class definition.

CLASS 726, INFORMATION SECURITY

Click here for a printable version of this file

SECTION I - CLASS DEFINITION

GENERAL STATEMENT OF THE CLASS SUBJECT MATTER

This class provides, within a computer or digital data processing system, for processes or apparatus for increasing a system s extension of protection of system hardware, software, or data from maliciously caused destruction, unauthorized modification, or unauthorized disclosure.

INFORMATION SECURITY

This class provides for protection of data processing systems, apparatus, and methods as well as protection of information and services. Subject matter included in this class includes security policies, access control, monitoring, scanning data, countermeasures, usage control, and data protection from maliciously caused destruction, unauthorized modification, or unauthorized disclosure. This class also includes protection of hardware, and user protection, e.g., privacy, etc.

SECTION II - REFERENCES TO OTHER CLASSES

SEE OR SEARCH CLASS:

326, Electronic Digital Logic Circuitry, subclass **8** for digital logic circuits acting to disable or prevent access to stored data or designated integrated circuit structure.

340, Communications: Electrical, subclasses **5.2** through **5.74**for authorization control without significant data process features claimed, particularly subclasses 5.22-5.25 for programmable or code learning authorization control; and subclasses 5.8-5.86 for intelligence comparison for authentication.

365, Static Information Storage and Retrieval, subclass **185.04** for floating gate memory device having ability for securing data signal from being erased from memory cells.

380, Cryptography, subclasses **200** through **242**for video with data encryption; subclasses 243-246 for facsimile encryption; subclasses 247-250 for cellular telephone cryptographic authentication; subclass 251 for electronic game using cryptography; subclasses 255-276 for communication using cryptography; subclasses 277-47 for key management; and subclasses 287-53 for electrical signal modification with digital signal handling.

455, Telecommunications, subclass **410** for security or fraud prevention in a radiotelephone system.

704, Data Processing: Speech Signal Processing, Linguistics, Language Translation, and Audio Compression/Decompression, subclass **273** for an application of speech processing in a security system.

705, Data Processing: Financial, Business Practice, Management, or Cost/Price Determination, subclass **18** for security in an electronic cash register or point of sale terminal having password entry mode, and subclass 44 for authorization or authentication in a credit transaction or loan processing system.

708, Electrical Computers: Arithmetic Processing And Calculating, subclass **135** for electrical digital

BMC EXHIBIT 2001
ServiceNow, Inc. v. BMC Software, Inc.; CBM2015-00170

710, Electrical Computers and Digital Data Processing Systems: Input/Output, subclasses **36** through **51**for regulating access of peripherals to computers or vice-versa; subclasses 107-125 for regulating access of processors or memories to a bus; and subclasses 200-240 for general purpose access regulating and arbitration.

711, Electrical Computers and Digital Processing Systems: Memory, subclass **150** for regulating access to shared memories, subclasses 163-164 for preventing unauthorized memory access requests.

713, Electrical Computers and Digital Processing Systems: Support, subclasses **150** through **181**for multiple computer communication using cryptography; subclasses 182-186 for system access control based on user identification by cryptography; subclass 187 for computer program modification detection by cryptography; subclass 188 for computer virus detection by cryptography; and subclasses 189-194 for data processing protection using cryptography.

714, Error Detection/Correction and Fault Detection/Recovery, subclasses **1** through **57**for recovering from, locating, or detecting a system fault caused by malicious or unauthorized access (e.g., by virus, etc.).

SECTION III - GLOSSARY

ACCESS CONTROL

The prevention of unauthorized access to resources of a system or information system, including the prevention of their use in an unauthorized manner.

INFORMATION

Data with meaning concerning a particular act or circumstance in general. Note: May include or consist of graphics or text or numerical or non-numerical values.

MONITORING

Subject matter includes means of watching, tracking, inspecting, analyzing of system or user activity. This includes the auditing of system vulnerabilities and system configuration, assessing the integrity of files within a system, identifying and recognizing patterns that dictate known attacks, analysis of abnormal activity patterns, recognizing user activity in regards to policy violations and operating system audit trail management.

POLICY

Rules for protecting information, services and other data processing resources.

USAGE CONTROL

Subject matter includes means placing restrictions on computer and/or user use of applications

USER PROTECTION/PRIVACY

Subject matter includes means for ensuring the state or integrity of information or data associated with a user.

SUBCLASSES

1 **POLICY:**
This subclass is indented under **the class definition**. Subject matter comprising systems, methods, and apparatus that provide for the administration and management of rules or regulations governing the protection of information, services and other data processing resources involving coordination of more than one security mechanisms among a plurality of entities, resources, or processes.

2 ACCESS CONTROL OR AUTHENTICATION:

This subclass is indented under the class definition. Subject matter comprising systems, methods, and apparatus for the prevention of unauthorized access to resources of a system or information system, including the manner of identifying and verifying the entity, process, or mechanism requesting access to the resource.

(1) Note. This subclass is directed to access control in information security systems. The concept of access control exists throughout the class. Therefore, a search to a particular concept of access control should consider the related topics in bus access control, memory access control, computer system access control, generic access control, etc.

SEE OR SEARCH THIS CLASS, SUBCLASS:

27, for prevention of unauthorized use of data access control.

SEE OR SEARCH CLASS:

340, Communications: Electrical, subclasses **5.8** through **5.86**for selective electrical communications systems with intelligence comparison for identity authentication.

345, Computer Graphics Processing and Selective Visual Display Systems, subclasses **716** through **726**for operator interface aspects of workgroup data processing environments for plural users or sites.

380, Cryptography, appropriate subclasses for systems employing encrypted user or record actuated authentication, and for digital control or digital computer communication in which an encrypting or decrypting device utilizes a digital signal manipulation technique on the computer signal, and subclasses **247** through **250**for cellular telephone cryptographic authentication.

705, Data Processing: Financial, Business Practice, Management, or Cost/Price Determination, subclass **18** for an electronic cash register having cryptography; and subclass 44 for a general funds transfer or credit transaction requiring authorization or authentication not including a cryptographic limitation.

707, Data Processing: Database, Data Mining, and File Management or Data Structures, subclasses **705** through **789**for database accessing and control.

709, Electrical Computers and Digital Processing Systems: Multicomputer Data Transferring, subclass **225** for controlling which of plural computers may transfer data via a communications medium.

710, Electrical Computers and Digital Data Processing Systems: Input /Output, subclasses **107** through **125**for bus access regulating.

711, Electrical Computers and Digital Processing Systems: Memory, subclasses **147** through **153**for shared memory access and control, and subclasses 163-164 for access limiting and password use therein.

713, Electrical Computers and Digital Processing Systems: Support, subclasses **155** through **159**for central trusted authority authentication; subclasses 168-181 for particular communication authentication technique; and subclasses 182-186 for system access control based on cryptographic user identification.

3 Network:

This subclass is indented under subclass 2. Subject matter including means of limiting access to the resources of a system based on a network level.

(1) Note. The network level is computer-to-computer communication.

SEE OR SEARCH CLASS:

709, Electrical Computers and Digital Processing Systems: Multicomputer Data Transferring, subclass **22** controlling which of plural computers may transfer data via a

4 Authorization:

This subclass is indented under **subclass 3**. Subject matter including permitting the use of rights, privileges, and permissions in a network environment.

SEE OR SEARCH THIS CLASS, SUBCLASS:

18, for stand-alone authorization.

21, for access control or authentication.

5 Credential:

This subclass is indented under **subclass 3**. Subject matter including the existence of network data that can be used to establish the claimed identity of a principal including passwords, biometrics.

SEE OR SEARCH CLASS:

382, Image Analysis, subclass **115** for image analysis for personal identification (biometrics).

713, Electrical Computers and Digital Processing Systems: Support, subclass **186** for biometric acquisition.

902, Electronic Funds Transfer, cross-reference art collection 3, for biometric evaluation in electronic funds transfer.

6 Management:

This subclass is indented under **subclass 5**. Subject matter including means or steps for administering credentials, including specific techniques for creating the credentials.

SEE OR SEARCH THIS CLASS, SUBCLASS:

18, for stand-alone credential management.

7 Usage:

This subclass is indented under **subclass 5**. Subject matter including means or steps for using the credential to establish the identity of the bearer.

SEE OR SEARCH THIS CLASS, SUBCLASS:

20, for stand-alone credential usage.

8 Global (e.g., Single Sign On (SSO), etc.):

This subclass is indented under **subclass 5**. Subject matter whereby a single credential can be used to access a plurality of systems or resources.

9 Tokens (e.g., smartcards or dongles, etc.):

This subclass is indented under **subclass 5**. Subject matter whereby the credential includes a unique combination of bits used to confer transmit privileges to a computer on a local network.

SEE OR SEARCH THIS CLASS, SUBCLASS:

20, for stand-alone authorization.

SEE OR SEARCH CLASS:

380, Cryptography, subclass **229** for authentication in a video system using a record or token.

705, Data Processing: Financial, Business Practice, Management, or Cost /Price Determination, subclasses 65 through 69for secure transaction including intelligent token.

713, Electrical Computers and Digital Processing Systems: Support, subclasses 172 through 174for generic authentication using intelligent token in multiple computer communication.

10 Tickets (e.g., Kerberos or certificates, etc.):

This subclass is indented under subclass 5. Subject matter whereby the credential includes data used to indicate that the bearer is authorized for access.

SEE OR SEARCH CLASS:

713, Electrical Computers and Digital Processing Systems: Support, subclasses 156 through 158for computer network certificates, and subclass 175 for generation of a certificate.

11 Firewall:

This subclass is indented under subclass 3. Subject matter including a device installed between internal (private) networks and outside networks (public) and which protects the internal network from network-based attacks that may originate from the outside and to provide a traffic point where security constraints and audits may be affected.

SEE OR SEARCH CLASS:

370, Multiplex Communications, subclasses 351 through 430for multiplex communication routing absent cryptography.

705, Data Processing: Financial, Business Practice, Management, or Cost /Price Determination, subclass 79 for cryptographic remote charge determination of a secure transaction including payment switch or gateway.

709, Electrical Computers and Digital Processing Systems: Multicomputer Data Transferring, subclasses 238 through 244for computer-to-computer data routing.

713, Electrical Computers and Digital Processing Systems: Support, subclasses 153 and 154 for a particular node in cryptographically protected multiple computer communication.

12 Proxy server or gateway:

This subclass is indented under subclass 11. Subject matter including an intermediate internetworking device that connects one or more networks to another for a specific application.

(1) Note. The gateway runs a process at the request of the client/user and obtains the service of a particular server; hence it works as both a client and a server provider.

13 Packet filtering:

This subclass is indented under subclass 11. Subject matter including a multi-ported internetworking device that applies a set of rules to each incoming IP packet in order to decide whether it is to be forwarded or dropped.

(1) Note. The filtering usually takes place on information contained in the headers, such as protocol numbers, source or destination addresses/ports, TCP connections, and other options. The filtering may be dynamic or static.

(2) Note. The packet filter may be different and distinct from routers; see note on routers. Routers are internetworking devices that run a custom operating system to transfer packets between two or more physically separated network segments (via the use of routing tables). This device operates at the network level of the OSI model, or the Internet level of the Internet model.

(3) Note. Some routers have a scanning ability and are know as screening routers, effectively becoming a packet-filtering device.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.