



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : H04L	A2	(11) International Publication Number: WO 00/08793 (43) International Publication Date: 17 February 2000 (17.02.00)
(21) International Application Number: PCT/US99/17647 (22) International Filing Date: 4 August 1999 (04.08.99) (30) Priority Data: 09/129,467 4 August 1998 (04.08.98) US (71)(72) Applicants and Inventors: SENATOR, Steven, T. [US/US]; 8625 Westminster Drive, Colorado Springs, CO 80920 (US). MULLIGAN, M., Geoff [US/US]; 2175 Cloverdale Drive, Colorado Springs, CO 80920 (US). BLUMENTHAL, John [US/US]; 4432 East Emigration Canyon, Salt Lake City, UT 84018 (US). (74) Agents: STRINGHAM, John, C. et al.; Workman, Nydegger & Seeley, 1000 Eagle Gate Tower, 60 East South Temple, Salt Lake City, UT 84111 (US).		(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>Without international search report and to be republished upon receipt of that report.</i>
(54) Title: APPARATUS AND METHOD FOR FORMING A PACKAGED-OBJECT PRODUCT AND A PACKAGED-OBJECT PRODUCT FORMED THEREFROM (57) Abstract An encapsulated object, and apparatus and an associated method for forming an encapsulated object, is formed of an object to which executable code is added. The executable code defines one or more policies, and a set of capabilities is associated with each policy. Compliance with the policy must be achieved prior to carrying out of an action upon the object.		

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

APPARATUS AND METHOD FOR FORMING A PACKAGED-OBJECT PRODUCT AND A PACKAGED-OBJECT PRODUCT FORMED THEREFROM

The present invention relates generally to object-oriented communication techniques and constructs. More particularly, the present invention relates to a packaged-object product. The present invention also relates to a method and apparatus for packaging a data payload with
5 executable code to form the packaged-object product. The executable code defines at least one policy, and a set of capabilities is associated with each policy. The policy responds to events which are associated with the capabilities.

The packaged-object product created according to an embodiment of
10 the present invention forms an encapsulated object having active, self-enforcing policies. When an encapsulated object is received at a receiving station, such as a computer, requests are made of the capability at the receiving station. The encapsulated object responds to the requests in a manner such that the policy, or policies, defined by the executable code are
15 enforced.

In an exemplary implementation, the data payload forms a digital data file, such as an e-mail document or facsimile document. The executable code packaged together defines at least one policy with which a capability is associated. The policy embodied by the executable code defines who, when,
20 or how a capability can be performed upon the data file. An exemplary policy embodied by the executable code comprises a restriction to access to the data file, and an exemplary capability includes a read capability to permit reading of the data file if compliance with the policy is achieved.

BACKGROUND OF THE INVENTION

25 Advancements in digital technologies have permitted the development of, and practical implementation of, a wide array of devices for performing

tasks which can be carried out at rates dramatically more quickly than that which can be performed manually. Devices utilizing digital technologies are typically able to perform repetitive functions at significant speeds. Because of the speed at which such functions can be performed, activities previously
5 considered impractical can now be readily implemented.

Devices used in a digital communication system are exemplary of devices which make use of some of such advancements in digital technologies. A communication system includes a sending station and a receiving station interconnected by way of a communication channel.

10 When the communication system is a digital communication system, the information which is to be transmitted between the sending and receiving stations is typically in the form of, or is represented by, binary bits. The binary bits are transmitted upon the communication channel to be received by the receiving station. Depending upon the characteristics of the
15 communication channel, binary bits forming the information might first be converted into a form to permit their transmission upon the communication channel. And, the receiving station must be able to receive and re-convert the converted-bits into a form to permit the informational content thereof to be recreated at the receiving station.

20 Advancements in digital technologies have also permitted the creation of, and affordability of, personal computers. Personal computers increasingly are used as communication devices to form portions of a digital communication system. Separate computers are connected together by way of private networks as well as by way of the internet. Data generated, or stored,
25 at one computer can readily be transmitted to another computer by way of network interconnections. E-mail documents, text documents, picture documents, and audio documents are all exemplary of information communicated between computers, or other digital processing devices.

Many other types of communication systems similarly make use of
30 digital technologies to communicate information between a sending station

and a receiving station. For example, facsimile machines also permit the communication of information between a sending-facsimile machine and a receiving-facsimile machine, typically connected together by way of a PSTN (public-switched telephonic network). A document which is to be transmitted is converted into digital form and a binary representation of the document is transmitted by the sending-facsimile machine to a receiving-facsimile machine. Digitized information can analogously be communicated between a sending and a receiving station of other types of communication systems.

Security issues relating to data communicated between a sending and a receiving station is sometimes of concern. Security of the communications is sometimes of concern, not only during transmission of information upon a communication channel but also subsequent to its reception at a receiving station. Encryption techniques, for example, are sometimes utilized to encrypt information prior to its transmission upon a communication channel to a receiving station. Encryption of the information reduces the possibility that a recipient, other than an intended recipient, shall be able to recover the informational content of the information. When received at a receiving station, the received information is de-encrypted, and thereafter, the informational content of the information is recovered. Once the information has been de-encrypted, the sender of the information no longer controls access to the information.

More generally, once the information is sent by a sender, the sender loses use-control over the information. If, however, the sender were able to maintain use-control over the information, the sender would be able to limit access to, and use of, the information.

A manner by which better to provide a sender of information greater use-control over the information subsequent to its communication to a receiving station would be advantageous.

It is in light of this background material related to the communication of information that the significant improvements of the present invention have evolved.

SUMMARY OF THE INVENTION

5 The present invention, accordingly, advantageously provides apparatus, and an associated method, for packaging a data payload together with executable code to form a packaged-object product. The executable code defines a policy with which compliance must be achieved to permit a capability, such as a read or copy operation, to be performed upon the data
10 payload.

The present invention further advantageously provides a packaged-object product formed of a data payload and executable code which defines a policy and with which a capability is associated. The policy responds to events which are associated with the capability.

15 In one aspect of the present invention, the packaged-object product forms an encapsulated object having active, self-enforcing policies. When such an encapsulated object is provided to an appropriate receiving station, requests are made of the capability associated with the executable code forming a policy and which is included as a portion of the encapsulated object.
20 The encapsulated object responds to the requests made of the encapsulated object at the receiving station. The responses are made in a manner such that the policy defined by the executable code is enforced. The executable code forming the policy defines who, when or how a capability can be performed. And, the capability associated with the policy defines an act which can be
25 carried out upon the object.

One or more policies are defined by the executable code and each policy has associated therewith one or more capabilities. That is to say, a set of capabilities is associated with each policy. An act carried out upon an object is dependent upon the requests made upon the encapsulated object by

the receiving station. Thereby, separate acts might be performed upon the encapsulated object dependent upon the requests made of it by the receiving station. Through use of appropriate policies, access to the object can be made to be limited. Security problems associated with an object subsequent to its de-encryption are obviated due to the self-enforcing nature of the policies of the encapsulated object.

The executable code defining the policy of the encapsulated object is formed of objects-oriented codes, such as JAVA™ code. An encapsulated object of an embodiment of the present invention is able to implement the specified policies which have associated therewith dynamics capabilities.

In an exemplary implementation, the packaged-object product includes a digital data file, such as an e-mail document, facsimile document, text file, picture file, or digitized audio file. The policy embodied by the executable code with which the data file is packaged defines who, when, or how a capability, such as a read capability, is performed upon the data file.

In another aspect of the present invention, the policy packager, and an associated method, packages data within at least one policy to form a packaged-object product. At least one policy is stored at a storage location of a storage element. Each policy has a set of capabilities associated therewith. Each capability of the set of capabilities is effectuable responsive to compliance with the policy to which the set of capabilities is associated. An adder is coupled to receive the data and to the storage element. The adder selectively accesses the storage location at which the policy is stored. The selected policy is retrieved and added to the data to package the data therewith. The data, once packaged with the selected policy, forms the packaged-object product.

In these and other aspects, therefore, a packaged-object product, and an apparatus and method for producing such product, is provided. The packaged-object product includes a data payload. At least one policy is packaged together with the data payload. The at least one policy defines selected

criteria and has associated therewith a set of capabilities. Each capability of the set of capabilities defines an event capable of being performed upon the data payload when compliance with the selected criteria defined by the policy is achieved.

- 5 A more complete appreciation of the present invention and the scope thereof can be obtained from the accompanying drawings which are briefly summarized below, the following detailed description of the presently-preferred embodiments of the invention, and the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

- 10 Figure 1 illustrates a functional block diagram of a policy packager of an embodiment of the present invention.

Figure 2 illustrates a representation of an encapsulated object of an embodiment of the present invention formed during operation of the policy packager shown in Figure 1.

- 15 Figure 3 illustrates a representation of a portion of the encapsulation layer of the encapsulated object shown in Figure 2.

- Figure 4 illustrates a functional block diagram of a communication system in which an encapsulated object, such as the encapsulated object shown in Figure 2, is generated and transmitted between a sending and a
20 receiving station.

Figure 5 illustrates a method flow diagram listing the method acts of the method of operation of an embodiment of the present invention.

DETAILED DESCRIPTION

- Referring first to Figure 1, a policy packager, shown generally at 10, is
25 operable to package an object 12 forming a digital payload together with one or more policies to form an encapsulated object 14. In an exemplary implementation, the policy packager is formed of a digital processor, such as a personal computer or other computing device. In such an implementation, the

objects 12 may also be generated at the digital processing device. The object 12 is here represented as an input to the policy packager 10 as, in the exemplary implementation, the object 12 is separately created and then applied to the policy packager 10.

5 The policy packager 10 is here shown to be coupled to a user interface. In an implementation in which the policy packager 10 forms a portion of a personal computer, the user interface 16 forms a computer key board permitting a user to enter input commands to effectuate operation of the policy packager, as appropriate. A controller 18 is operable to control packaging
10 operations of the packager 10 and is here shown to be coupled to receive commands generated by way of actuation of the user interface 16.

 The policy packager 10 is further shown to include a storage element 22 having a plurality of storage locations 24. In the implementation in which the policy packager is embodied by a computer, the storage elements 22 is
15 formed alternately of computer main memory or storage elements of a computer-peripheral, storage device. Data stored in the storage locations of the storage elements 22 form executable code defining policies. Each policy has associated therewith a set of one or more capabilities. Each policy defines
20 who, when or how a capability can be performed. And, each capability defines an action.

 The policy packager further includes an adder 26 coupled to receive the object 12 and also to data stored in storage locations 24 of the storage element 22. Operation of the adder 26 is here shown to be controlled by the controller 18 which is also operable to control which of the data stored in the selected
25 ones of the storage locations is provided to the adder 26. The adder 26 is operable to package together the objects 12 and one or more policies formed of the data stored in the storage locations 24 of the storage element. The adder forms the encapsulated object 14 by packaging together the objects 12 together with the data forming the policies retrieved from the storage locations
30 24. Selection of which of the policies is added by the adder 26 together with

the object 12 is made by user actuation of the user interface 16 or can be automatically selected by way of an automated process. The adder 26 is operable, for example, to concatenate together an object 12 to the data forming the selected policies.

5 In one implementation, the data payload forming the object 12 forms a facsimile document, and the policy packager 10 forms a portion of a facsimile machine. In another implementation, the data payload forming the object 12 comprises an e-mail document, such as that generated at a personal computer, and the policy packager 10 forms a portion of such personal computer. In an
10 analogous manner, the data payload forming the object 12 can also be formed of any digital material, such as digitized text, digitized picture information, and digitized audio information. The policy packager 10 forms a portion of digital processing apparatus operable to receive and perform operations upon such digital data.

15 Figure 2 illustrates an encapsulated object 14 of an embodiment of the present invention. The encapsulated object 14 forms a packaged-object product, such as that formed by the policy packager 10 shown in Figure 1. The encapsulated object 14 is formed of a data payload, here the object 12. Exemplary objects 12 include facsimile documents, e-mail documents, text
20 documents, digitized picture documents, digitized audio documents, and the like. The encapsulated object 14 also includes executable code forming one or more policies 32. While in an actual implementation, the executable code forming policies 32 are concatenated together with the objects 12. Policies 32 are here shown to be packaged about, or to encapsulate, the objects 12. Such
25 encapsulation indicates that the access to the objects 12 is limited, and the policies 32 form a self-enforcing, content-control mechanism which limits the performance of actions upon the object unless compliance with at least one, more than one, or all of the policies 32 is achieved. The exemplary object 14 shown in Figure 2 includes N policies which encapsulate the object 12. N can
30 be of any selected number.

A set of capabilities is associated with each policy 32. A policy defines who, when or how, an action can be performed upon the objects 12. The capability defines the action which can be performed upon the object if the policy with which the capability is associated is complied with, the capability can be performed upon the objects 12.

Figure 3 illustrates the policies 32, and sets 34 of capabilities 36 associated with the policies 32. In an exemplary implementation, the executable code of which the policies 32 are formed comprise object-oriented code, such as JAVA TM code. Exemplary capabilities 36 associated with various of the policies include, for example, a read capability, a forward capability, a change (or overwrite) capability, an append capability, an annotate capability, and a delete-object capability.

Both the policies and the capabilities associated with the policies are dynamically-selectable during creation of the object, such as by the policy packager 10 shown in Figure 1. Each policy 32 forms a content-control mechanism controlling access to the objects 12 to have one or more capabilities performed thereon.

An exemplary encapsulated object includes a text document forming the object 12 and which includes a legal notice message. The document forming the object 12 is encapsulated with a policy of: a presentation of the legal notice to a prospective-accessor, and legal notice acknowledgment, or a failure to do so. A capability associated with such policy permits limited access to the document if the prospective-accessor acknowledges retrieval of the legal notice. Such an encapsulated object limits access to the document unless a prospective accessor acknowledges receipt of the legal notice associated with the document.

Figure 4 illustrates a communication system, shown generally at 52, having a transmitting station 54 and a receiving station 56, interconnected by way of a communication channel 58. In an exemplary implementation, the transmitting and receiving stations 54 and 56 form computer stations

connected together by way of a computer network which forms the communication channel 58. The transmitting station 54 includes a policy packager 10 and, here, also an object creator 62. The object creator 62 creates an object 12 (shown in Figure 1). The object created by the object creator 62 is provided to the policy packager 10 which packages the object together with one or more policies as above-described to form an encapsulated object 14 (shown in Figures 1 and 2). Additional portions (not shown) of the transmitting station 54 place the object 14 in a form to permit its communication upon the networked connection 58 for transmission to the receiving station 56.

The receiving station 56 receives the encapsulated object 14 transmitted upon the network 58. The encapsulated object is delivered to an area of the receiving station 56 at which requests are made of the capabilities associated with the at least one policy of the encapsulated object. The receiving station generates events, also referred to as method requests or messages, and the encapsulated object responds to such events. The object responds to the events in manners which enforce the policy or policies of the encapsulated object. When compliance is achieved with the policy or policies, performance of the one or more capabilities associated with such policy or policies is carried out at the receiving station.

Figure 5 illustrates a method, shown generally at 72, of an embodiment of the present invention. The method 72 packages a data payload within at least one policy to form a packaged-object product.

First, and as indicated by the block 74, at least one policy is stored. The policy has a set of capabilities associated therewith. Each capability of a set of capabilities is effectuable responsive to compliance with the policy with which the set of capabilities is associated. Then, and as indicated by the block 76, one or more policies stored during the act of storing is selectively accessed.

Thereafter, and as indicated by the block 78, the policy accessed during the act of selectively accessing is retrieved. And, as indicated by the block 82, the policy retrieved during the act of retrieving is added to the data payload. Thereby, the data payload is packaged with the policy. The data
5 payload, once packaged with the policy forms the packaged-object product.

Thereby, through operation of an embodiment of the present invention, self-enforcing content control is provided to an object. The creator and sender of the encapsulated object of an embodiment of the present invention thereby includes active, self-enforcing policies. When an encapsulated object is
10 received at a receiving station, effective control over the object is maintained by the creator by virtue of the policies packaged together with the object.

The previous descriptions are of preferred examples for implementing the invention, and the scope of the invention should not necessarily be limited by this description. The scope of the present invention is defined by the
15 following claims:

We claim:

1. A packaged-object product receivable at a receiving station, said packaged-object product comprising:
 - a data payload; and
 - at least one policy packaged together with said data payload.
- 5 said at least one policy defining selected criteria, and said at least one policy having associated therewith a set of capabilities, each capability of the set of capabilities defining an event capable of being performed upon said data payload when compliance with the selected criteria defined by said policy is achieved.
2. The packaged-object product of claim 1 wherein said at least one policy comprises executable code.
3. The packaged-object product of claim 2 wherein each capability of the set of capabilities associated with said policy forms an interface to the executable code of which said policy is comprised and to said data payload.
4. The packaged-object product of claim 1 wherein the receiving station includes a user actuator actuatable by a user, and wherein the compliance with the selected criteria defined by said policy is determined responsive to user actuation of the user actuator.
5. The packaged-object product of claim 1 wherein the receiving station includes at least one characteristic associated therewith, wherein the selected criteria defined by said policy pertains to a receiving-station characteristic, and wherein compliance with the selected criteria defined by
5 said policy is achieved wherein the characteristic associated with the receiving station corresponds with the receiving-station characteristic formed of the selected criteria.
6. The packaged-object product of claim 1 wherein said at least one policy comprises a first policy and at least a second policy, said first policy

defining first selected criteria and said at least second policy defining second selected criteria, said first policy having associated therewith a first set of capabilities and said at least second policy having associated therewith a second set of capabilities.

7. The packaged-object product of claim 1 wherein said set of capabilities associated with said policy comprises a first capability and at least a second capability, said first capability defining a first event and said at least second capability defining at least a second event.

8. The packaged-object product of claim 1 wherein said data payload comprises a digital work.

9. The packaged-object product of claim 8 wherein the receiving station comprises a facsimile machine and wherein said data payload comprises a facsimile document.

10. The packaged-object product of claim 8 wherein the receiving station comprises digital processing apparatus capable of receiving an e-mail document and wherein said data payload comprises an e-mail document.

11. The packaged-object product of claim 8 wherein the receiving station comprises digital processing apparatus capable of receiving a text file and wherein said data payload comprises a text file.

12. The packaged-object product of claim 8 wherein the receiving station comprises digital processing apparatus capable of receiving a picture-document and wherein said data payload comprises a picture-document.

13. The packaged-object product of claim 8 wherein the receiving station comprises digital processing apparatus capable of receiving a digitized-audio document and wherein said data payload comprises a digitized audio-document.

14. The packaged-object product of claim 1 wherein a capability of the set of capabilities associated with said at least one policy comprises a read capability.

15. A policy packager for packaging data within at least one policy to form a packaged-object product, said policy packager comprising:

5 a storage element having at least one storage location for storing at least one policy, each policy stored thereat having a set of capabilities associated therewith, each capability of the set of capabilities effectuable responsive to compliance with the policy to which the set of capabilities is associated; and

10 an adder coupled to receive the data and to said storage element, said adder for selectively accessing the at least one storage location at which the at least one policy is stored for retrieving a selected policy of the at least one policy stored at said storage element, and for adding the selected policy to the data to package the data therewith, the data, once packaged with the selected policy, forming the packaged-object product.

16. The policy packager of claim 15 wherein said storage element comprises a computer memory of a computer system.

17. The policy packager of claim 16 wherein said adder comprises a computer processor of a computer system.

18. The policy packager of claim 15 further comprising a user actuator coupled to said adder, said user actuator actuatable by a user to cause accessing of the storage location of said storage element by said adder.

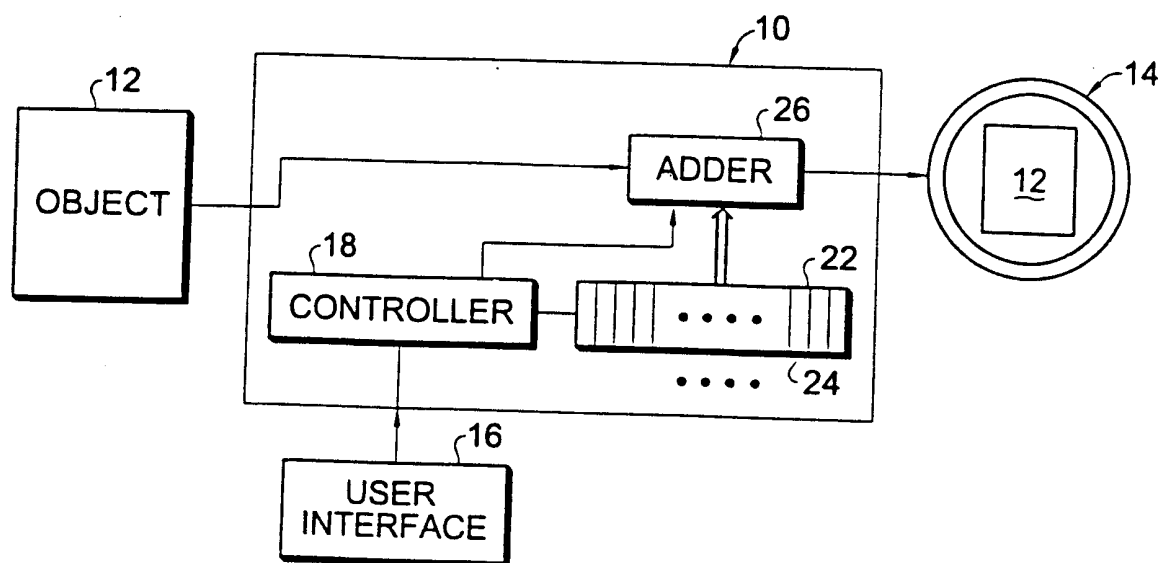
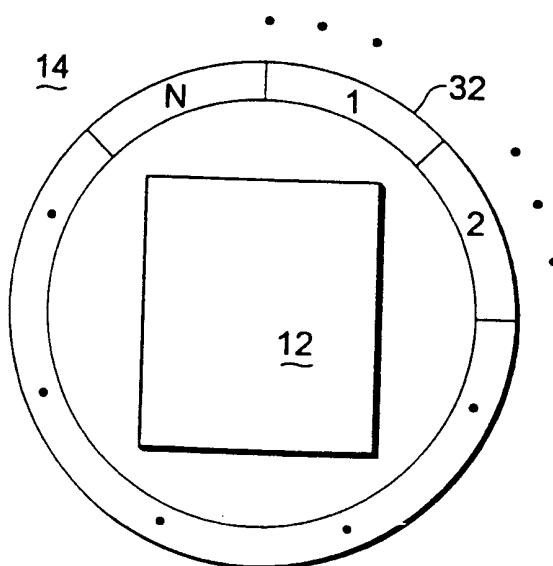
19. A method for packaging data payload within at least one policy to form a packaged-object product, said method comprising the acts of:

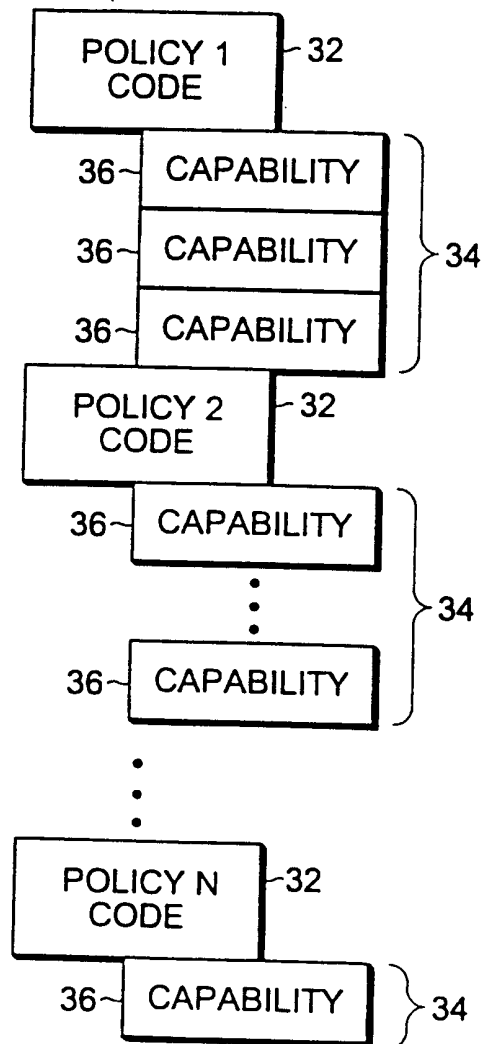
5 storing at least one policy having a set of capabilities associated therewith, each capability of the set of capabilities effectuable responsive to compliance with the policy with which the set of capabilities is associated;

selectively accessing a policy of the at least one policy stored during said act of storing;

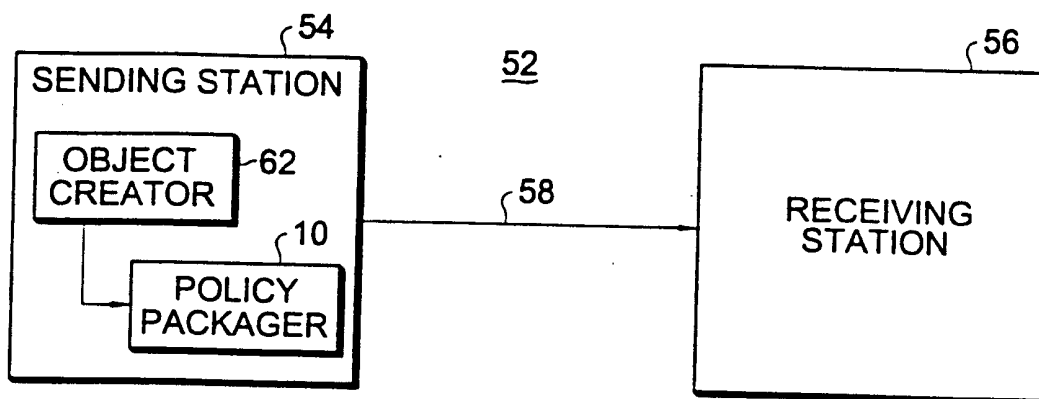
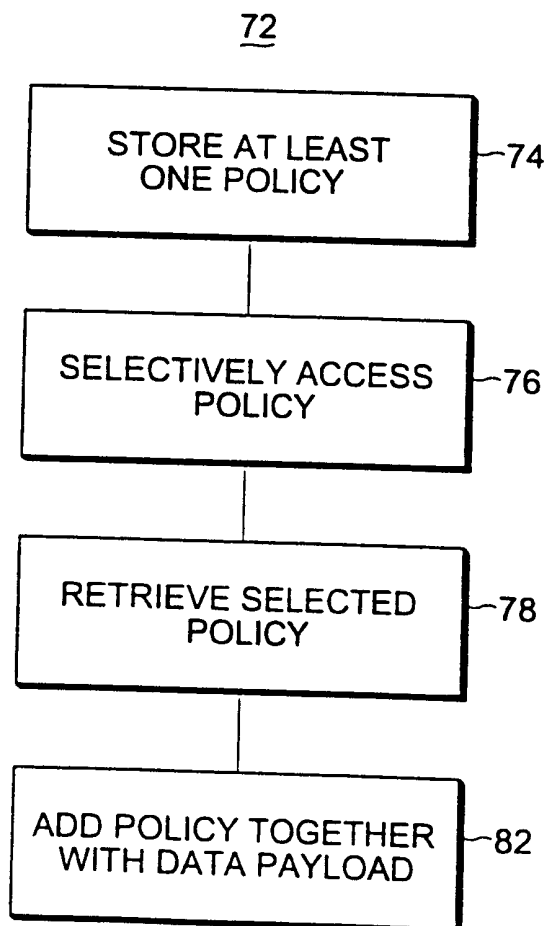
retrieving the policy accessed during said act of selectively accessing; and

10 adding the policy retrieved during said act of retrieving to the data payload to package the data payload therewith, the data payload, once packaged with the policy, forming the packaged-object product.

*FIG. 1**FIG. 2*

*FIG. 3*

3/3

*FIG. 4**FIG. 5*