

A SYSTEM FOR DIVERSIFYING INFORMATION IN A NETWORK FOR
DISTRIBUTING GOODS OR SERVICES

The present invention relates to a system for
diversifying information conveyed by a network to
5 apparatuses that deliver goods or services.

A particularly advantageous application of the
invention is in the field of secure electronic transaction
systems such as payment systems, mobile-telephone networks,
computer networks, pay-television systems, etc.

10 Goods or services distribution networks comprise one or
more platforms, also called network heads, which are
essentially computer systems, PC or mainframe computers,
responsible for creating messages, on the order of the
operator in charge, each message being sent via a
15 transmitter device to the various apparatuses connected to
the network under consideration.

By way of example, the messages can include information
relating to authorizing the user of the destination
apparatus to access a product or a service such as a payment
20 service, a telephone service, access to computer functions
(bulletin board or software downloading), or access to
encrypted television programs. Conversely, said platforms
can also issue messages for removing previously-granted
access rights, or even for modifying such rights, in
25 particular after they have been extended to new products or
services proposed by the network to its subscribers.

The messages transmitted by the platforms are picked up
by a receiver in each apparatus and then forwarded to a
security module present in each apparatus, the purpose of
30 said module being to control access via the corresponding
apparatus to the products or services distributed by the
network.

The security modules, referred to herein as "access
control modules", can be detachable from the apparatus, e.g.
35 an electronic memory card or the like, or non-detachable
therefrom, e.g. a security component.

Since the platforms allow the access rights of the apparatuses to the various goods or services of the network to be created, modified, or taken away, the messages issued therefrom must be completely secure.

5 To this end, in order to prevent any previously-recorded access-authorization message from being reissued to an apparatus by a pirate transmitter after access authorization has been taken away, diversification systems can be used, for example. Similarly, it is necessary to
10 prevent a message intended for one apparatus from being diverted to another apparatus.

A known diversification system consists in including diversification data in each message created by the platforms, which data is combined by means of an encrypting
15 algorithm with a secret key belonging to each platform, thereby enabling a message certificate or signature to be created. In order to prevent a message intended for one apparatus from being diverted to another apparatus, instead of using the secret key of the platform in order to build up
20 the certificate, use is made of a diversified secret key resulting from another encrypting algorithm combining the secret key of the platform with an identification number of the destination access control module.

Since the access control module of the destination
25 apparatus of the message also knows both the secret key of the platform and the encrypting algorithm, it can in turn reconstruct the certificate and compare it with the transmission. If the comparison is positive, it can be concluded that the transmitter which sent the message does
30 indeed have the secret key and that the message has not been modified.

As in said diversification system, the diversification data must belong to each message, and when there are two or more platforms, they must be synchronized, either by being
35 connected to a single diversification-data generator which distributes diversification data on demand from the

platforms, or by each having its own generator with reporting to the other generators for each message.

The diversification data can be a random number provided by a random number generator. In that case, and in
5 order to avoid any message duplication, the access control modules must be able to store the random numbers of all of the messages that they receive, in order to be able to verify that a random number received has not been received previously, which would mean that the message has already
10 been received. To do that, it is necessary to reserve a large amount of space in the access control module. For example, with each message having a 4-byte random number, 4000 reserved bytes are required for 1000 messages, that being half the memory space normally available in access
15 control modules.

To remedy that drawback, diversification data can be used which is constituted by the serial number of the transmitted message, which serial number is generated by a message counter which increments by unity with each message
20 transmitted by any of the platforms of the network. It thus suffices for the access control modules to store the number of the last message received and to verify that said number is greater than the previously received number.

However, a drawback to that system is that, in the
25 event of unexpected stoppage, it is necessary to restart the counter from number 1, which would lead to any new message being rejected since it would be considered as a prior message and therefore as having already been received. In that case, a safeguard means would be for each access
30 control module to store the numbers of all the messages received, but the problem thus arises of the cost of the safeguard.

Thus, a first technical problem to be solved by the present invention is to eliminate the constraints associated
35 with synchronizing platforms in a system for diversifying information carried by a network to apparatuses that deliver goods or services, said network including a plurality of

platforms each capable of creating messages including diversification data for diversifying the information to be carried, said diversification data being provided by respective diversification-data generators, and each
5 apparatus including a respective access control module.

According to the present invention, the solution to this first technical problem consists in that each platform has an autonomous diversification-data generator, and in that said access control module of each apparatus includes,
10 firstly, storage means for storing the diversification data conveyed with the last message issued by each platform, and secondly, comparison means for comparing each new value of the diversification data received from each platform with the previous value, at least.

15 Thus, the access control modules of the network have as many storage means as the network has platforms, each storage means being assigned to the diversification-data generator of a respective platform.

Because the diversification-data generators are
20 autonomous, the platforms no longer need to be synchronized, thereby greatly simplifying the network, and the small increase in the number of storage means in the access control modules is not a severe penalty.

Another technical problem that the invention also
25 proposes solving, is that of enabling the platforms to become operational again after failure, while still maintaining maximum security.

To this end, according to the invention, said diversification-data generator is a universal time base,
30 said diversification data being, for example, the transmission date of the message relative to a known arbitrary origin t_0 .

In the event of a platform breaking down (assuming the origin t_0 is not lost) the system can restart at a date
35 which is later than the date of the last message provided by said platform. Thus, no special safeguard needs to be envisaged.

Finally, with a view to reducing the size of the storage means in the access control modules, the invention provides for said time base to have a duration t_{max} limited to not less than the lifetime of said access control

5 modules. In other words, instead of sizing the storage means in terms of the lifetime of the network, e.g. 40 years, they are sized for a lifetime that is only slightly greater than the lifetime of the modules, e.g. 10 years.

10 However, a problem arises for modules which are put into operation a short time before t_{max} has elapsed since, theoretically, they will no longer be able to accept messages after said date, the time base being reset to zero and any new messages thus presenting an apparently earlier date.

15 In order to solve this difficulty, the invention provides discrimination means consisting in that each access control module stores in memory the transmission date t_1 of the first message provided by each platform, and in that validation of a message transmitted at a date t_{n+1} is
20 performed by comparing the transmission date t_1 with the transmission date t_n of the previous message:

if $t_n > t_1$ the message at t_{n+1} is validated if t_{n+1} is not included in $]t_1, t_n[$

25 if $t_n < t_1$ the message at t_{n+1} is validated if t_{n+1} is included in $]t_n, t_1[$.

In this way, the access control modules can be used during the entire duration t_{max} , whatever the date on which they are put into operation.

30 The invention and implementation thereof will be well understood from the following description, given by way of non-limiting example and with reference to the accompanying drawings.

Figure 1 is a diagrammatic view of a goods and services distribution network of the invention provided with a system
35 for diversifying information.

Figure 2 is a diagram showing how a message provided by the platforms of the network of Figure 1 is built up.

Figure 3 is a diagram giving the structure of the access control modules of the apparatuses of the network of Figure 1.

Figure 4 is a timing diagram of a time base used as a generator for generating diversification data for the platforms of Figure 1.

The diagrammatic view of Figure 1 shows a goods and services distribution network comprises a plurality, N , of platforms PF1, PF2, ..., PFk, ..., PFN capable of responding to instructions from the network operator OP by creating messages MS1, MS2, ..., MSk, ..., MSN intended for a plurality, M , of apparatuses AP1, AP2, ..., APj, ..., APM subscribing to the network, such as mobile telephones for example. Said messages MSk are conveyed to the various apparatuses by transmitter devices EM1, EM2, ..., EMk, ..., EMN each associated with a respective platform.

Messages MSk are received by apparatuses APj and conveyed to access control modules MODj with which said apparatuses are respectively equipped. Before taking account of the information contained therein, the access control modules are responsible for authenticating and validating the messages received, e.g. access authorization or even modification or removal of previously-granted access rights.

Figure 2 shows the typical structure of a message MSk intended for an apparatus APj. Said message, referenced here as MSk,j includes the information proper INFk to be conveyed to apparatus APj. It also includes diversification data DDK provided by an autonomous diversification-data generator GENk, belonging to platform PFk. Said platform PFk is also given its own secret key KSk. Each access control module MODj is assigned an identification code IDj, and the entire set of identification codes is known to each platform. Thus, when a platform PFk needs to provide a message MSk,j for apparatus APj, a diversified secret key KDK,j is built up from the secret key KSk, the information INFk, and the identification code IDj by an encrypting

algorithm which can be of the DES type or more simply an exclusive-OR. The diversified secret key KDk,j is combined with the diversification data DDk by means of another encrypting algorithm, DES for example, to constitute a
5 certificate $CERk,j$.

By diversifying the secret key relative to the destination module $MODj$, the diversification system is able to prevent a message addressed to one apparatus from being used for another.

10 As can be seen in Figure 3, module $MODj$ of apparatus APj has the secret keys KSk of each platform Pfk stored in memory. On receiving the message, it can in turn compute a certificate in the same way as platform Pfk and verify the authenticity of message MSk,j by comparing the certificate
15 thus computed with the certificate $CERk,j$ appearing in said message.

As a way of eliminating any need for synchronization between platforms Pfk to prevent the various platforms from sending messages MSk having the same diversification data DDk , and as shown in Figure 3, the access control modules $MODj$ include means STk for storing the value of the
20 diversification data DDk conveyed with the last message MSk provided by each platform Pfk . Since the diversification data is stored separately for each platform, there is no
25 longer any danger of collision and therefore no longer any need for synchronizing the platforms with one another, they thus become autonomous: in addition, each module $MODk$ is provided with means for comparing each new value of the diversification data DDk received from each platform Pfk
30 with the previous value, at least, so as to prevent a message that has already been sent, and in particular an access authorization, from being stored and resent to the apparatus in fraudulent manner after access authorization has been taken away by the operator OP .

35 As mentioned above, the diversification data DDk can be random numbers provided by a random number generator $GENk$. However, in order to avoid any repetition, it is necessary

to store all the random numbers received via each platform in the access control module.

In this case, any new random number received is compared with all those already received from the same
5 platform.

The serial number of the messages received from each platform PF_k , which increments by unity for each new message, can also be used for diversification data. The diversification-data generator GEN_k is thus merely a
10 counter. In each module MOD_j , the storage means ST_k record the number DD_k of the last message transmitted by the platform PF_k . For the following message issued from the same platform PF_k , the access control module verifies that the number DD_k+1 of the new message is indeed subsequent to
15 DD_k , in which case the message can be validated. Said diversification system has the advantage of requiring only a single data item to be stored in said storage means.

The invention also proposes another type of diversification-data generator, the principle of which is
20 shown in Figure 4.

It relates to a generator constituted by a universal time base for which the diversification data DD_k is the transmission date t_k of the message, said date being taken relative to a known arbitrary origin t_0 . In the event of
25 the platform stopping unexpectedly, it is able to restart operating automatically since t_0 is not lost. Thus, no special safeguard has to be provided.

In order to limit the size of the storage means ST_k , the time base can, instead of being given a duration t_{max}
30 equal to the lifetime of the network, e.g. 40 years, be limited to a duration slightly longer than the average lifetime of the access control modules MOD_j . In this case, the diversification data DD_k of platform PF_k returns to zero after having reached t_{max} .

35 It is thus understood that, without special precautions, the access control modules would reject any messages received after the date t_{max} , whatever the date t_1

at which the module was put into operation, since the diversification data DDK is apparently lower than the previous data. This means that modules which have been manufactured and stored long after the date t_0 have a
 5 considerably shortened working lifetime.

This is why discrimination means are provided which allow that drawback to be avoided. These means consist in that each module MODj stores in memory the transmission date t_1 of the first message MS1 provided by each platform, the
 10 validation of a message transmitted at a date t_{n+1} being performed by comparing the transmission date t_1 with the transmission date t_n of the previous message in the following way:

if $t_n > t_1$ the message at t_{n+1} is validated if t_{n+1} is not
 15 included in $]t_1, t_n[$

if $t_n < t_1$ the message at t_{n+1} is validated if t_{n+1} is included in $]t_n, t_1[$.

As shown in Figure 4, the lifetime of the modules can thus be extended beyond t_{max} until $t_{max} + t_1$ giving a full
 20 working duration of t_{max} .



CLAIMS

- 1/ A system for diversifying information (INF_k) carried by a network to apparatuses (AP_j) that deliver goods or services, said network including a plurality of platforms (PF_k) each
5 capable of creating messages (MS_k) including diversification data (DD_k) for diversifying the information (INF_k) to be carried, said diversification data being provided by respective diversification-data generators (GEN_k), and each apparatus (AP_j) including an access control module (MOD_j),
10 said system being characterized in that each platform (PF_k) has an autonomous diversification-data generator (GEN_k), and in that said access control module (MOD_j) of each apparatus (AP_j) includes, firstly, storage means (ST_k) for storing the value of the diversification data (DD_k) conveyed with the
15 last message (MS_k) issued by each platform (PF_k), and secondly, comparison means for comparing each new value of the diversification data (DD_{k+1}) received from each platform (PF_k) with the previous value (DD_k), at least.
- 20 2/ A diversification system according to claim 1, characterized in that said diversification-data generator (GEN_k) is a random-number generator.
- 3/ A diversification system according to claim 1,
25 characterized in that said diversification-data generator (GEN_k) is a message counter.
- 4/ A diversification system according to claim 1, characterized in that said diversification-data generator
30 (GEN_k) is a universal time base.
- 5/ A diversification system according to claim 4, characterized in that the diversification data (DD_k) is the transmission date t_n of the message (MS_k) relative to a
35 known arbitrary origin t_0 .



6/ A diversification system according to claim 4 or 5, characterized in that said time base has a duration t_{max} limited to at least the lifetime of said access control modules (MODj).

5

7/ A diversification system according to claim 6, characterized in that each access control module (MODj) stores in memory the transmission date t_1 of the first message (MS1) provided by each platform (PFk), and in that
10 validation of a message (MSk+1) transmitted at a date t_{n+1} is performed by comparing the transmission date t_1 with the transmission date t_n of the previous message (MSk):

if $t_n > t_1$ the message at t_{n+1} is validated if t_{n+1} is not included in $]t_1, t_n[$

15 if $t_n < t_1$ the message at t_{n+1} is validated if t_{n+1} is included in $]t_n, t_1[$.