Title: A TICKET AND A METHOD OF BILLING

Abstract: The invention relates to a method of attaching a billing ticket (22) to a transfer protocol such as HTTP for communication over an open network (10) for data and telecommunication between an end-user (14), a service provider (12) and a content provider (18), and a ticket (22) therefore.
Published:
--- with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
Title

A ticket and a method of billing

Technical field

The present invention pertains to a method of attaching a billing ticket to a transfer protocol for communication over an open network for data and telecommunication between an end-user, a service provider and a content provider, and a ticket therefore.

Background art

The growth of the Internet, the World Wide Web, and associated services, has as businesses mature come to a point where there is an urge to enable content providers to be able to charge an end-user for value-added services, such as on-line media, recruiting, intellectual property based services etc.

There is a strong feeling for that businesses would have to close if they start to charge for their contents, as end-users will stop use their services, this mainly because it does not exist a suitable or practical method of billing. It is not doubted that the growth of the Internet and the popularity of services largely depend on an accessibility aspect. Every attempt to add additional complicated steps to a communication diminishes a “click-and-go” feeling, which should be a signature of the web.

Requesting Internet visitors/end-users to specify credit-card numbers has many drawbacks, for example, the fact that the cost for transactions tend to be high, often higher than the cost for the service itself, and the obstacles and discomfort added tend to scare end-users away.

Other attempts to sign up customers into an account, where a periodic billing comprises summing up costs during a specified timeframe is problematic due to remote identification and authentication problems. Still other methods include additional costs and obstacles of installing hardware and/or software in a client computer.

In particular, seldom visited services, such as for instance services for travellers who would like to be presented a weather forecast from a local newspaper’s site in a country to be visited, is a type of service that is likely to be used only once, or at least only very few times. The cost and administrative undertaking in supporting vast numbers of small customers, potentially all over the world is simply not practically feasible.

Initiatives for a tax-like system have been considered for an implementation in network operators and Internet service provider systems, in order to receive revenue streams to the content providers. Apart from an apparent threat that service providers would reject requests to such sites, such a revenue billing scheme is likely to be considered unfair from a
service provider's point of view. Moreover, as the web is worldwide by its nature, intra-regional and intra-continental billing is unlikely to be practically feasible for an implementation.

In telephone networks, there exists an established infra-structure of a service provider having an established relationship with a customer and payment routines to adequately charge customers linked to a fixed account. Furthermore, value-added services can be charged through the telephone operator, whereby a calling prefix, "toll number", routes the caller to a service that is charged separately from the ordinal telephone rate. Weather forecasts, horoscopes, computer support, charity etc. have successfully implemented a working business model, where customers are willing to pay for services, as there is a convenient method of payment, included on the monthly telephone bill.

A similar model for customers using services on the Internet, without the need to change an end-user's computer environment, would be appreciated.

Summary of the invention

The present invention aims to solve the problems mentioned and presents a reliable method for a transfer protocol and a ticket for the same. Hence the present invention sets forth a method of attaching a billing ticket in a transfer protocol for a communication requested by an end-user over an open network for data and telecommunication through at least one service provider to a content provider. The invention is comprising:

in the transfer protocol an identity to a provider of services or content, the ticket comprising at least, a time stamp, a counter and a random number;

a message authentication code attached to the ticket, which verifies the validity of the ticket at a provider of services or content when successfully decoded; and

the counter counting time periods in addition to the time stamp, thus making possible to differ between tickets with time stamps issued at a same time period.

In one embodiment it is provided a cost code field for a requested services is added to the ticket.

In another embodiment of the present invention it is further comprising:

storing content providers universal resource locator in a list in a database at the service provider, which indicates if a requested service is charged at the content provider;

the service provider intercepting and analysing a transfer protocol data name server query for a requested universal resource locator, performing a look-up in the database for an indicated charge for the requested universal resource locator;
buffering a response to the requesting end-user if the requested universal resource locator is charged; and
transferring the end-user request with attached ticket and message authentication code to the content provider.

Still another embodiment comprises:
the content provider receiving an end-user request; and
transferring the end-user request with identity and attached first ticket and message authentication code to the service provider;
the service provider analysing the identity and verifying the message authentication code, performing a look-up in a database for an indicated charge for the requested universal resource locator;
the service provider sending a message with at least the first ticket with content provider identity and a second ticket issued by the service provider, the service provider identity, and message authentication code; and
upon an accept by the end-user of the requested services, the message being sent to the content provider verifying the first ticket and identity and the service provider identity, second ticket and message authentication code, whereby a successful verification initiates a requested end-user services.

A further embodiment provides that a request from an end-user to be provided an universal resource locator to a content provider residing in the network of a different service provider than its own, the service providers issuing and checking tickets between themselves with their identifiers before clearing a connection to the sought content provider.

A still further embodiment comprises that an end-user not registered to utilize the method, requesting an universal resource locator to a content provider, is being redirected to an advertising home page in the network to be informed about the method.

Still another embodiment provides that each issued ticket has a limited lifetime of being in a pending state.

Yet one embodiment comprises that an internet service provider holds a list of ticket timeout values for different content providers.

Yet another embodiment comprises that a non-responding content provider request rejected by the end-user or content providers, will provide a ticket timeout, hindering a billing to be recorded.

A yet further embodiment provides that the counter is incremented at each access request, and reset at each current universal time coordinated timestamp increment.
Yet still a further embodiment provides that the ticket is a long arbitrary number, represented as a linear sequence, a random sequence or a combination of both.

To achieve the aims and goals of the present invention it further sets forth a billing ticket in a transfer protocol for a communication requested by an end-user over an open network for data and telecommunication through at least one service provider to a content provider. The ticket thus comprises:

in the transfer protocol an identity to a provider of services or content, the ticket comprising at least, a time stamp, a counter and a random number;

a message authentication code attached to the ticket, which verifies the validity of the ticket at a provider of services or content when successfully decoded; and

the counter counting time periods in addition to the time stamp, thus making possible to differ between tickets with time stamps issued at a same time period.

One embodiment of the ticket comprises that a cost code field for requested services is added to the ticket.

Another embodiment provides that the counter is incremented at each access request, and reset at each current universal time coordinated timestamp increment.

A further embodiment provides that the ticket is a long arbitrary number, represented as a linear sequence, a random sequence or a combination of both.

**Brief description of drawings**

Henceforth reference is had to the following description and its accompanying drawings with examples and embodiments for a better understanding of the present invention, in which:

**Fig. 1** schematically illustrates a customer to content provider relationship over the Internet;

**Fig. 2** schematically illustrates ISP identifier and a ticket in accordance with the present invention;

**Fig. 3** schematically illustrates CP identifier and a ticket in accordance with the present invention;

**Fig. 4** schematically illustrates an ISP approval ticket in accordance with the present invention; and

**Fig. 5 and 6** schematically illustrate a ticket in accordance with the present invention for an intra content payment.
Description of preferred embodiments

In a simplified customer to content-provider relationship schematically depicted in the attached Fig. 1, an end-user 14 conventionally connects to the Internet 10 through an Internet 10 service provider (ISP) 12, typically a telephone- or network operator. Connection can either be performed through a switched fixed-network (PSTN, Public Switched Telephone Network; Integrated Services Digital Network, ISDN; x (generic) Digital Subscriber Line, xDSL) or through a fixed connection. These different connection types generally share the characteristic that there is a service provider, which acts as a gateway between a customer and the Internet 10. Independently if the connection is made from a person residing in its residential home, or over a high-capacity line, through a corporate LAN gateway 16, the service provider 12 can identify the connection to a specific end-user 14 account.

Provided, as an example, is a residential end-user 14 that connects to a CP 18 (Content Provider) site. The end-user 14 logs on through an Internet 10 browser and enters the Universal Resource Locator (URL) of the CP 18, in this example the URL http://www.xxx.com. Technically, this takes place through a HyperText Transfer Protocol (HTTP) GET/POST operation, requesting a response from the requested CP 18 controlled server, through the routing mechanisms of the ISP 12 and the Internet 10. The CP 18 is not able to reliably identify neither the ISP nor the end-user 14, but has enough information to pass the requested information back to the requesting end-user 14.

In accordance with the present invention, the ISP 12 intercepts all request operations of end-users 14 and performs a lookup of the URL. The lookup table, not shown, holds all URL of available CP 18, which the ISP 12 has established a billing agreement with. If the URL is found in the table list, the ISP 12 attaches a tag/ticket 22 to the request, containing, with reference to Fig. 2, an ISP 12 Identifier (SPIID 20), a “ticket 22”, within a bracket in Fig. 2, intended for a single use, and a Message Authentication Code (MAC), not shown. In one embodiment of the present invention, the ticket 22 is typically a long arbitrary number, either represented as a linear sequence, a random sequence or a combination of both. It is vital that two identical tickets 22 should not occur, to prevent a playback operation or tampering with the ticket 22. A playback operation is prevented by a time stamp 24 comprised in the ticket 22 of the present invention by using values from a system clock providing the actual system time. The counter 26 provides accuracy, for example, if two tickets 22 are produced within the same UTC time stamp 24.
Hence, the present invention provides the ticket 22 in the transfer protocol an identity 20 to a provider of services 12 or content, whereby the ticket 22 comprises at least, a time stamp 24, a counter 26 and a random number 28. Also provided is a message authentication code attached to the ticket 22, which verifies the validity of the ticket 22 at a provider of services 12 or content 18 when it has been successfully decoded. The counter 26 is counting time periods in addition to said time stamp 24, thus making possible to differ between tickets 22 with time stamps 24 issued at a same time period.

Implementation of MAC is the result of a cryptographic operation, operating on the SPID 20 identifier and ticket 22, using a secret key, shared by an ISP 12 and a CP 18. The encryption billing scheme can either be symmetric, i.e. the ISP 12 and CP 18 holds the same secret key, or having an asymmetric key pair, where the ISP 12 typically holds the private and the CP 18 the public key.

The receiving CP 18 is able to analyse each HTTP GET/POST request and check for such a tag/ticket 22 and to verify an added SPID 20, ticket 22 and MAC in accordance with the present invention to determine if the end-user 14 is to be granted or rejected access to the service.

The HTTP response, which is sent back to the client/end-user 14 through the ISP 12, contains the ticket 22, charging amount, in a currency specified by the ISP 12 CP 18 list, and a MAC. The ISP 12 is able to use a lookup table, not shown, to match the received ticketed with the list of issued tickets 22 to determine which account is to be charged, and which CP 18 is to receive the charged amount. After the response has been analysed, the information is removed, and a clean response (the HTML page sent is stripped of billing information) is sent to the client/end-user 14.

ISP 12 and CP 18 can periodically match their respective lists of tickets 22, sorted per ISP 12 and CP 18 to clear the balance due. This process could be automated.

In one embodiment of the present invention, the approach is, instead of rejecting a request with a missing ticket 22, to redirect the request to an advertising page, encouraging the end-user 14 to contact its ISP 12 to establish an agreement with the CP 18. Another option is to let the end-user 14 attend a limited free service. Although a more sophisticated billing scheme could be applied, where the first access to a certain CP 18 would pass back a request to the ISP 12 that this is a charged service, this would result in longer response time and additional network overhead.

Depending on the agreement between an ISP 12 and a CP 18, different rules may apply of how to notify an end-user 14 that it is being charged for access to contents. A
straightforward model is to notify the end-user 14 each time through a dialog, where the end-user 14 is notified, for example, in accordance with “This service will be charged with $0.20 to your ISP 12 account. Press OK to accept, CANCEL to reject.”. State-of-the art models of using cookies, or hidden fields in HTML documents may apply to automatically control a granting process for maximum end-user 14 convenience.

In order to avoid invalid charging in cases where the response to a client/end-user 14 is disrupted, the CP 18 should implement a billing scheme to keep the ticket 22 only when all data has been sent to the client. Furthermore, the ISP 12 is able to add additional features of removing billing tickets 22 if a communications failure occurs.

Each issued ticket 22 practically has a limited lifetime in a pending state, as the response from the CP 18 is normally expected in seconds or less. The ISP 12 can in one embodiment hold a list of ticket 22 timeout values for different CP 18, probably including information of expected peak times. Non-responding CP 18 or requests rejected by the end-user 14 or CP 18, will provide a ticket 22 timeout, which hinders any billing recordings.

As long as the encryption keys held by the ISP 12 and CP 18 can be managed in a secure fashion and a strong MAC the present invention is difficult to tamper with, thus avoiding fraud access. Any attempt to access the CP 18 directly, bypassing a valid ISP 12, results in the CP 18 rejecting the request, as there is no valid ticket 22 present. Attaching invalid tickets 22 will also fail, as the authenticity of the ticket 22 is validated using the MAC.

One further aspect of the billing scheme, is that the ISP 12 at any time can exclude groups of end-users 14 to access certain CP 18. Further, a CP 18 can at any time reject requests from a specific ISP 12, and an ISP 12 can at any given time entirely remove an entry from the list of valid CP 18. Unreliable, or potential offensive CP 18, can be instantly controlled by the ISP 12.

Another aspect of the present invention is that the ISP 12 can hold a credit limit for individual end-users 14, automatically rejecting further requests until the end-user 14 has paid its outstanding debt. Other billing schemes may include specific end-users 14 to prepay a retainer in order to use charged services. In a similar fashion, a CP 18 can reject requests from an ISP 12, exceeding their credit limits.

The billing scheme of the ISP 12 is similar to an ordinary telephone network access as well as the usage of toll numbers, where the subscription itself is the identity for billing, rather than a specific end-user 14. This means, that any end-user 14 accessing a CP 18 from a specific subscription account, will result in that the owner of the account is charged.
This corresponds to a family having telephone access, where the ISP 12 must include a non-repudiation statement in the terms of use for a customer.

A more sophisticated implementation would allow individual end-users 14 to explicitly enable only a specific CP 18, or group of CP 18. Moreover, end-users 14 can be allowed to explicitly block a specific CP 18 or groups of CP 18. An ISP 12 is able to categorize a CP 18 into different groups, allowing end-users 14 to access or block specific content categories, where a typical scenario includes an account holder allowing family or employee access to education, financial or weather sites and disabling games, violence and pornographic sites.

Furthermore, several different models may apply between end-users 14 and ISP 12, between ISP 12 and CP 18, and even between end-users 14 and CP 18. An ISP 12 may have special tariff agreements with a specific CP 18, thus enabling billing structures between ISP 12 and CP 18 to be different from the billing structures between an end-user 14 and a CP 18. For example, a large national ISP 12 may have special agreements with the ISP 12 top-ten most visited CP 18, where a fixed billing rate applies, whereas the ISP 12 charges end-users 14 for each used ticket 22.

A different approach to an ISP-CP relationship regards a larger company, where employees access the Internet 10 via a Local Area Network (LAN) through a corporate Internet 10 gateway 16. Implementing ISP 12 software as a proxy server, either on that gateway, or externally, could achieve the same functionality as previously described. In this case, the grouping of CP 18 could be used to prevent employees to access non-business critical services. With such an approach companies are able to establish a corporate to CP 18 subscription of, for example, an on-line version of a financial news service.

Although not different from a conceptual viewpoint, multiple CP 18, sharing single IP numbers, such as CP 18 located at a Web hosting server, have to be handled slightly different. In that case, the relative path, or URI, of the HTTP GET/POST operation has to be analysed as well, in extension to the DNS query.

A potential caveat from a CP 18 point of view is the presence of proxy servers caching static content information. Apart from the CP 18 inserting expiration and cache-control information in HTTP headers, the ISP 12-CP 18 relationship may apply different rules how this condition is to be handled and compensated.

Although the present invention is described with the use of the HTTP protocol, it can be implemented on other Internet 10 protocols, like file transfer protocol (FTP) or post office protocol 3 (POP3). It is, however, a crucial requirement, that the protocol itself is not
modified. Nor must extensions that may interfere with analysing routers, such as firewalls, be used.

In the following text a scenario is described where an end-user 14 connects to the Internet 10 via an Internet 10 Service Provider 12, utilizing a dial-up connection. An end-user 14 is going to visit a specific Content Provider 18 site on the Internet 10, using a web browser. Technically, this request results in two operations, a Domain Name System (DNS) query and a HyperText Transfer Protocol (HTTP) GET/POST operation. The DNS query translates the end-user 14 URL into an Internet 10 Protocol (IP)-address, which more efficiently identifies the queried resource on the Internet 10. Large sites on the Internet 10 may have several IP numbers mapped to a single URL, resulting in a different IP number for subsequent DNS queries.

A following HTTP GET/POST operation uses a retrieved IP number to address the CP 18, where the request is routed through the ISP 12 and the routing mechanisms of the Internet 10, ending up at the CP 18 server. The CP 18, practically unaware of both the ISP 12 and the end-user’s identities, processes the request and sends a response back to the requesting end-user 14.

In accordance with an embodiment of the present invention, the ISP 12 holds a list of CP 18, where each CP 18 is a part of a business relationship with the ISP 12. The list, for each CP 18, further contains a list of URLs that are non-free services.

The ISP 12 intercepts and analyses each incoming DNS query, and performs a lookup in a table to determine if the requested URL is free to use or not. If the URL is found in the list, the IP response is buffered in a list linked to the requesting end-user 14.

The destination IP address of each HTTP GET/POST operation is intercepted and analysed by the ISP 12. For each request having an IP number present in the end-user’s IP list, the ISP 12 attaches a tag/ticket 22 to the request, containing a ISP 12 Identifier (SPID 20), a single-use "ticket 22" and a Message Authentication Code (MAC). The ticket 22 is provided a UTC time stamp 24 of, in this embodiment 32 bits, a microsecond counter of 24 bits and a random number 28 of 40 bits.

The SPID 20 is an identifier, uniquely identifying the ISP 12. Using one IP number held by the ISP 12, ensures its uniqueness by using a established and regulated infrastructure of issuing unique identifiers, rather than establishing one new for this purpose.

The ticket 22 constitutes in one embodiment of the invention a per ISP 12 and per CP 18 unique, long arbitrary number, uniquely identifying a request sent from the ISP 12 to the CP 18. Current Universal Time Coordinated (UTC) time 32, a microsecond counter 26,
and a random number 28 are concatenated into a 96 bit identifier, serving as a unique and statistically variant ticket 22. A system without a reliable microsecond counter 26 could use a lower resolution sub-second counter and pad out unused bits with random number. As mentioned the counter 26 adds time to a UTC time stamp 24 in order to be able to differ between requests by end-users that have received the same UTC time stamp in their tickets 22.

The SPID 20 and ticket 22 are concatenated into a 128-bit value.

The MAC is a cryptographic checksum of the SPID 20 and ticket 22, used by the CP 18 to verify the integrity of these entries. The MAC algorithm used is AES encryption of the 128-bit SPID 20 and ticket 22, using a 128 bit symmetric key, resulting in a 128-bit cipher text. Although asymmetric encryption schemes have obvious benefits in terms of non-repudiation, the AES is used to achieve highest performance versus encryption strength ratio. The extra payload now added to the request is $128 + 128$ bits, and is appended as content in the HTTP request.

The CP 18 receiving the packet is now able to check the presence of the ticket 22, determine if the ISP 12 is valid, verify the MAC and either reject or accept the request from the end-user 14. Recording the SPID 20 and ticket 22 together with a billing code serves as the basis for the CP 18 billing the ISP 12.

In order to ensure end-user 14 confidence for the method of the present invention, a billing scheme has to be implemented so that the end-user 14 is notified that the service is about to be charged for. An amount, and clear instructions and selection of how to proceed or cancel will be presented before the response is sent, and the ticket 22 is saved by the CP 18 for billing.

In one scenario, the CP 18 records an accepted ticket 22, and associated charging information is periodically sorted and batch-wise transferred to the respective ISP 12, so that the CP 18 can receive its outstanding debt.

One-way billing, as described above, holds an obvious caveat in terms of risk for both the CP 18 and ISP 12. Insolvent end-users 14 may lead to the ISP 12 being forced to pay the CP 18 for usage, resulting in an economic loss for the ISP 12. Insolvent ISP 12 may lead to credit-losses for CP 18.

A method of enhancing the billing scheme to address the concerns described involves adding a second-level ticket 22 to each response, holding charging information, where the ISP 12 is able to analyse and strip the response packets for tickets 22. This method
would allow the ISP 12 to constantly monitor outstanding balance, and, when appropriate, reject end-user 14 requests when a specified credit limit has been reached.

In such a scenario, the ISP 12 can implement a second-level of billing scheme, independently of the CP 18. The end-user 14 logging to an ISP 12 account and view current balance on-line. The ISP 12 can further recalculate billing information into local currencies for maximum end-user 14 convenience.

Although primarily intended for virtual services, such as on-line newspapers, magazines, music, chat-rooms, pictures, health information, financial information, statistics, horoscopes etc., it is likely to be useful for ordering of low-cost physical items, such as fast food, flowers, newspapers, lottery ticket 22, commuter ticket 22 etc.

Other services, like on-line betting, charity, aid is as well potential targets of usage.

In dependence of the ethical profile of the ISP 12, the ISP 12 can freely decide to classify each connected CP 18 by its own judgment, in terms of dependability, category, offensiveness, objectivity, political, social and religious values etc. The ISP 12 could instantly shut-down impolite, or potential offensive CP 18, as well as impolite end-users 14.

An ISP 12 can also implement an end-user 14-accessible control panel, where settings filtering out certain type of content providers and further set maximum charge amount per week, per transaction, credit limits etc.

Several scenarios may apply in terms of business relationships between end-users 14 and ISP 12, between ISP 12 and CP 18 and between end-users 14 and CP 18. An obvious example is a large national newspaper having a fixed-monthly fee for access to its on-line services by a large national ISP 12. The ISP 12 could then either enable access to that newspaper as a part of its services to its customers, or add a second level of billing to end-users 14, independent of the agreement between the ISP 12 and the CP 18.

Also, ISP 12 may include a fixed free amount of content into their fixed monthly fee. Different end-users 14 may also have different credit limits. New end-users 14, free-ISP 12 access end-users 14 etc. may need to insert a retainer in order to access content. When the retainer has been used up, further accesses are rejected until a new retainer has been paid.

Reference is no had to Fig. 3 schematically illustrating a CP 18 identifier and a ticket in accordance with the present invention. In this embodiment of the invention an end-user 14 requests a CP 18 service, which is charged. The CP 18 responds with an approval form, typically using Hyper Text Markup Language (HTML) page description language. The form contains invisible fields, holding information about the CP 18, the session and the cost
of the service. The default behaviour of the HTML form is that it displays a message that the service is unavailable, as there is no agreement in place with the end-user 14 ISP 12.

In more detail, the secret fields 24, 26, 28, 34 form a “ticket” 22, within bracket in Fig. 3, issued by the CP 18 is 256 bits in length, and contains the following information.

The CPID 30 is an identifier, uniquely identifying the content provider.

Practically, this could be an Internet Protocol 10 (IP) number held by the CP 18, as central authorities issue them, guaranteeing their uniqueness. For CP 18 not having a fixed IP number, a central authority may issue phantom IP-numbers to uniquely identify the SP. A fraudulent CP 18, issuing an invalid IP-number, potentially resulting in a clash, will not affect the security of the system, as is shown obvious below.

The UTC timestamp 24 is a one second resolution timestamp in this embodiment, taken from a reasonably reliable time source of the CP 18 server computer. A practical requirement is that the timestamp 24 should not ever move backwards over any specified amount of time.

The Linear counter 26 is used to guarantee uniqueness for tickets 22 issued at the same second or other possible time period. The counter 26 is incremented at each access, and reset at each UTC 24 timestamp increment.

A cost code 34 describes a CP 18 to ISP 12 defined cost for an issued request.

The Random number 28 is used to add statistical variance to the ticket 22. It is desirable that the random number algorithm is not deterministic, as that would allow an alien to issue invalid future tickets 22, with high probability of not being detected.

MAC as mentioned is a cryptographic checksum of the CPID 30, UTC Timestamp 24, Linear counter 26 and Random number fields 28. Practically, this is implemented using AES encryption of these fields, using a secret key, shared by the CP 18 and ISP 12. Although obvious benefits exist in using asymmetric encryption for non-repudiation purposes, the symmetric 128-bit AES encryption is used to achieve high performance and encryption strength. An off-line attack against the MAC to find the secret key is not a practical threat, as the $2^{128}$ equally possible keys would take an enormous time in amount, even when hypothetically using millions of computers in parallel.

The ticket 22 forms a self-contained unique reference to the transaction, which can be verified by anyone sharing the secret key. Discussing protection and maintenance of the secret key is beyond the scope of this invention, although a possible method is presented below.
The CP 18 holds all issued tickets 22 in a list queue together with a timeout value, which when elapsed, discards the ticket 22 from the queue, considering the proposal is implicitly rejected. A ticket 22 is embedded as a hidden field, having a defined identity, such as “cpTicket” (cp= a code for the content provider) in a CP 18 issued response. The 256 bit binary value is encoded using Base64 encoding. Moreover, a response is designed to as default, for example, showing “Non-free service, request rejected (with the hidden field invisible to the end-user 14). Contact your ISP 12 for details”, as a form when utilizing a browser not modified by the ISP 12. The form also includes details for how the ISP 12 can sign up to the CP 18 and offer the CP 18 services to its customers.

Reference is now had to Fig. 4, which schematically illustrates an ISP approval ticket in accordance with the present invention. The ISP 12 monitors and analyses all received responses, searching for the presence of a hidden CP 18 ticket 22 field. If not found, or considered invalid, the response is passed unmodified to the requesting end-user 14.

The ISP 12 extracts the CPID 30 from the ticket 22 and searches for a matching entry in a list of CP 18, which the ISP 12 has a business agreement with. If not found, the response is passed unmodified to the requesting end-user 14. ISP 12 verifies the integrity of the ticket 22, by using a secret key for the found CP 18. If the result not matches, the response is passed unmodified to the requesting end-user 14. The ISP 12 now considers the ticket 22 to be valid for billing, and modifies the default behaviour of the form to an approval form. This is practically implemented by the ISP 12 replacing the entire CP 18 default form with an ISP 12 predefined approval form. The ISP 12 translates the cost code into a real cost in local currency terms, depending on the CP-ISP business models for billing. A form showing the cost, together with an ISP 12 defined classification description of the CP 18 and instructions how to accept the transaction and how to reject it, which is passed to the requesting end-user 14. The form further contains the CP 18 issued ticket 22 as a hidden field, invisible to the end-user 14. The ISP 12 keeps the pending approval information in a list queue, where each entry has a timeout and is discarded when a timer has elapsed.

An ISP 12 may also check the cost with an accumulated outstanding debt, and if appropriate, send a predefined “Request rejected, credit limit exceeded” form to the end-user 14.

A requesting end-user 14 can now decide if to accept or reject the proposal from the CP 18 and ISP 12. This is practically performed by pressing either an, for example, Windows® graphical “Accept” or “Reject” button or like. The proposal can also be rejected by simply not responding to it. In response, the end-users 14 selection is sent back to the ISP
12, typically using a submit HTTP POST operation. Its response to the ISP 12 is analysed for the end-users 14 selection, and if rejected, the form is passed back to the CP 18 unmodified.

If the end-user 14 accepts, the ISP 12 searches its list queue for the CP 18 issued ticket 22 and inserts an approval ISP 12 ticket 22 in the form having a layout in accordance with Fig. 4.

The ISPID 40 is an identifier, with the same characteristics as the CPID 30, with the difference that it identifies the ISP 12 rather than the CP 18. ISP 12 can either pass back the CP 18 cost code or modify it to reflect a different cost, defined by an agreed ISP-CP business model.

When the CP 18 receives the ISP-modified end-user 14 response, the CP analyzes the ISP 12 ticket 22 and verifies the ISP 12 and the ticket 22 authenticity in the same manner the ISP 12 verified the CP 18 ticket 22. The CP may, for different reasons, decide to reject the accepted proposal. Either if the credit limit of the ISP 12 has been exceeded, or the cost proposed by the ISP 12 is not acceptable by the CP 18.

CP 18 refers to its queued list with issued tickets 22 to verify that the received CP 18 ticket 22 has been correctly issued and not being timed out. Associated request data, stored with the queued ticket 22, is used to complete the end-user 14 content request.

Although some technical details have been left out for the sake of clarity, the billing scheme described shows a straight-forward implementation of an ISP 12 handled batch-wise billing method for maximum end-user 14 convenience.

An ISP 12 may, according to its own ethical, social and religious objectiveness, classify each CP 18 signing up for a business agreement into different categories, also setting a quality standard for each CP 18, which can be presented for the end-user 14 prior to accepting a proposal.

End-user 14 feedback about concerned CP 18 can be collected and moderated by the ISP 12, creating a "popularity factor". Together with this factor, the end-user 14 can review other end-user 14 experience of the CP 18 prior to accepting a CP 18 proposal, probably increasing end-user 14 confidences about accepting or rejecting proposals from unknown CP 18. The ISP 12 can further decide to terminate an agreement with a CP 18 receiving too many complaints from end-user 14.

Furthermore, the ISP 12 can assure end-user 14 confidence of the system, by allowing the end-user 14 to access a restricted private control panel page, where certain tasks can be automated and the end-user 14 personal preferences can be set, such as maximum allowed balance due, maximum purchases per day, per week etc.
Specific ISP 12 classifications can be enabled for access, such as financial
information, news and weather, where others, like violence, pornographic, and game sites can
be explicitly disabled or restricted for access. Restricted access may include ISP 12 initiated
warning messages, or ISP 12 verified password entry to accept a CP 18 proposal.

New end-users 14 or other groups of end-users 14 may, depending on the ISP 12
judgment, be required to pre-pay an initial retainer for access to billed services. When the
retainer has been exhausted, the ISP 12 will reject further access attempts until the retainer
has been restored to a preferred limit.

Several different business models may apply between end-users 14 and ISP 12,
between ISP 12 and CP 18 and also between end-users 14 and CP 18. Some ISP 12 may have
special tariff agreements with a specific CP 18, allowing billing structures between ISP 12
and CP 18 to be different from the billing structures between the end-users 14 and the CP 18.
For example, a large national ISP 12 may have special agreements with the SP’s top-ten most
visited CP 18, where a fixed billing rate applies, whereas the ISP 12 charges end-users 14 for
each used ticket 22. An ISP 12 may include a fixed free amount of content into their fixed
monthly fee. On-line charity and aid organizations can act as CP 18, enabling a highly
efficient method of collecting small funds, without the normal cost overhead involved.

Fig. 5 and Fig. 6 illustrate the ticket 22 of the present invention for an intra ISP
12 content payment. The fields in the ticket 22 correspond to those depicted in Fig. 3 and Fig.
4. In one embodiment it is assumed that the requested CP 18 service is not free of charge. The
CP 18 has a billing agreement with its ISP 12, i.e., the ISP2. When the page of non-free
content is requested, the CP 18 server normally responds.

In order to make a filtering process efficient, the CP 18 places non-free services
in a defined root catalogue, known by ISP2. Included in the HTTP request is a Universal
Resource Identifier (URI) part, which identifies the relative path of the root IP address
obtained from the DNS query. ISP2 analyses all incoming HTTP request to each CP 18 it has
billing agreements with and verifies the URI, using a CP 18 provided list, to determine if the
service is free to use or not.

If the root path is found, the ISP 12 intercepts the HTTP GET request and
responds with a default response to the requester, optionally including ISP2 and/or CP 18
clear-text defined advertising and content description, stating that the requested service is not
available, due to that there is no billing agreement in place between ISP1 and ISP2.
Embedded within the response is an invisible tag, such as a hidden field or a meta-tag, with an
ISP 12 issued “ticket” 22.
The ISPID2 50, in Fig. 5 is an identifier, uniquely identifying the ISP 12. Practically, this can be any Internet Protocol (IP) number held by ISP2, as central authorities issue them and guarantees their uniqueness. If required, a central authority may issue phantom IP-numbers to uniquely identify ISP2. Any fraudulent issuer, trying to masquerade the IP address of an ISP 12, will not affect the security of the system, as will be obvious from the present description. A default response, issued by ISP2, is addressed for requesters accessing through an ISP 12, which has no billing agreement with ISP1.

ISP2 analyses all incoming HTTP responses, and searches for the well-defined hidden field, holding a ticket 22. If an invalid, or no ticket 22 is found, the response is passed back, unmodified to the user. If ISP1 finds a valid ticket 22, i.e. the identity and layout matches, then ISP1 searches its list of known ISPs 12, to find out if it has a billing agreement with ISP2. If not, the response is passed back, unmodified to the user.

If ISP1 finds a valid billing agreement, it analyses the response and translates the cost-code into a cost in local currency, about to be billed to the user's ISP1 account. The actual cost is likely to be defined by an agreement between ISP1 and ISP2. This agreement may be different from the agreement between ISP2 and the CP 18. Further; ISP1 inserts a second ticket 22, similar to the one issued by ISP2.

The ISPID1D 60, in Fig. 6, equivalent in scope to ISP2ID, holds a unique identifier, identifying ISP1. Finally, ISP1 inserts information and functionality in a response form, including easy-to-understand information how to accept or reject the offer proposed by CP 18, ISP2 and ISP1. This is typically made, presenting a text like "This request will cost you $0.10, which will be charged to your [ISP1] account. Do you want to proceed?" followed by an "Accept" and a "Reject" button or the like. Pressing "Accept" will typically result in a HTTP submit POST operation being passed back to ISP2, through ISP1.

ISP2 analyses incoming requests and searches for a valid issued ticket 22 in its issued tickets list. Typically, each ticket 22 has a limited lifetime, where ISP2 discards all tickets older than, for example, three minutes. If either ISP1 or the user rejects the proposal, no response is being sent to ISP2, resulting in a ticket 22 timeout.

If a valid ISP2 ticket 22 is found, a search for an ISP1 ticket 22 is performed. If the ISP1 ticket 22 is found, ISP2 verifies if it has a billing agreement with ISP1, which is the most likely situation, as ISP1 would not issue a ticket 22 otherwise. If found, and verified correctly by ISP2, the request is passed back to the CP 18.

Several options may apply about how the actual billing and clearing process is performed. ISP1 may at any moment decide to terminate its agreement with ISP2, as it can
instantly determine the origin of the proposal, whereas the same applies to ISP2. A negotiation process may be initiated between ISP2 and ISP1, where the cost proposal of ISP2 may be modified by ISP1 and included in its ticket 22. ISP2 may decide if the proposal is to be accepted and rejected.

Furthermore, on-line account verification and clearing can be performed, as the cost of the request is known by each part. From ISP1’s point of view, a cost proposal can be verified by the user’s current balance due, and ISP1 may decide to reject it if the user’s credit limit is exceeded. If ISP1 analyses the acceptance HTTP post, it is able to on-line update the user’s current debt. From ISP2’s point of view, the same rules may apply, and ISP2 may decide to reject an approved proposal if ISP1’s outstanding debt is too high or overdue.

The clearance process between ISP2 and ISP1 may either be performed on-line or batch-wise, where both parties can verify their both lists of collected and issued tickets.

As a service to an end-user, a well-defined structure of content classification may be implemented, where each ticket 22 may be extended to hold a content descriptor, originally supplied by the CP 18. Each ISP 12 may decide to subclass each content class with information defining its own subjective classing, based on advertising content, objectiveness, offensiveness, violence content, social-, ethical- and cultural correctness etc. The receiving party may decide to rely on and to use that information or not.

An example: ISP2 classifies one CP 18 as “news”, “medium objectiveness”, “low offensiveness”, “Christian values”. ISP1 receives that information, and considers parts of the sub classing as “too subjective”, based on the own subjective classification of ISP2, but decides to keep “news” and “low offensiveness” as key elements, shown to the requesting user. ISP1 may decide to fully, or partly, automate its sub classing process, based on user feedback, reflecting the median values of its customer base. An automated “Customer feedback survey form” may voluntary collect information, automatically updating ISP1 records. The ISP2 sub-classification may in the same way be updated by feedback from ISP1 etc.

In a similar fashion, a CP 18 ranking and politeness service may be implemented, where complaints sent back from users to ISP1, automatically, or semi-automatically updates a “Customer rank” figure maintained by ISP1. This ranking may be presented to the user as a part of the approval process.

Summarising, the described invention creates a fundament for an easy to understand, hard to circumvent, implementation straightforward structure for billing with a minimum of obstacles for an end-user 14.
Although the present invention has been described through examples and preferred embodiments, the attached set of claims sets out further embodiments for a person skilled in the art.

---------
Claims

1. A method of attaching a billing ticket (22) in a transfer protocol for a communication requested by an end-user (14) over an open network (10) for data and telecommunication through at least one service provider (12) to a content provider (18), characterized by comprising:

in said transfer protocol an identity (20, 30, 40, 50, 60) to a provider of services (12) or content (18), said ticket (22) comprising at least, a time stamp (24), a counter (26) and a random number (28);

a message authentication code attached to said ticket (22), which verifies the validity of the ticket (22) at a provider of services (12) or content (18) when successfully decoded; and

said counter (26) counting time periods in addition to said time stamp (24), thus making possible to differ between tickets with time stamps issued at a same time period.

2. A method according to claim 1, characterized in that a cost code (34) field for a requested services is added to said ticket (22).

3. A method according to claims 1 or 2, characterized by further comprising:

storing content providers (18) universal resource locator in a list in a database at the service provider (12), which indicates if a requested service is charged at said content provider (18);

said service provider (12) intercepting and analysing a transfer protocol data name server query for a requested universal resource locator, performing a look-up in said database for an indicated charge for the requested universal resource locator;

buffering a response to the requesting end-user (14) if the requested universal resource locator is charged; and

transferring the end-user (14) request with attached ticket (22) and message authentication code to the content provider (18).

4. A method according to claims 1-2, characterized by further comprising:

said content provider receiving an end-user (14) request; and

transferring the end-user (14) request with identity (30) and attached first ticket (22) and message authentication code to said service provider (12);
said service provider (12) analysing the identity (30) and verifying the message authentication code, performing a look-up in a database for an indicated charge for the requested universal resource locator;

said service provider sending a message with at least said first ticket with content provider (18) identity (30) and a second ticket issued by the service provider (12), the service provider identity (40), and message authentication code; and

upon an accept by the end-user (14) of the requested services, said message being sent to said content provider (18) verifying the first ticket (22) and identity (30) and the service provider identity (40), second ticket (22) and message authentication code, whereby a successful verification initiates a requested end-user (14) services.

5. A method according to claim 3, characterized in that a request from an end-user (12) to be provided an universal resource locator to a content provider (18) residing in the network of a different service provider (12) than its own, the service providers issuing and checking tickets (22) between themselves with their identifiers (50, 60) before clearing a connection to the sought content provider (18).

6. A method according to claims 1-4, characterized in that an end-user (14) not registered to utilize the method, requesting an universal resource locator to a content provider (18), is being redirected to an advertising home page in the network to be informed about the method.

7. A method according to claims 1-5, characterized in that each issued ticket (22) has a limited lifetime of being in a pending state.

8. A method according to claim 7, characterized in that an internet service provider (12) holds a list of ticket (22) timeout values for different content providers (18).

9. A method according to claims 1-5, characterized in that non-responding content provider (18) request rejected by the end-user (14) or content providers (18), will provide a ticket (22) timeout, hindering a billing to be recorded.

10. A method according to claims 1-9, characterized in that said counter (26) is incremented at each access request, and reset at each current universal time coordinated (24) timestamp increment.

11. A method according to claims 1-10, characterized in that the ticket (22) is a long arbitrary number, represented as a linear sequence, a random sequence or a combination of both.
12. A billing ticket (22) in a transfer protocol for a communication requested by an end-user (14) over an open network (10) for data and telecommunication through at least one service provider (12) to a content provider (18), characterized in that it comprises: in said transfer protocol an identity (20, 30, 40, 50, 60) to a provider of services (12) or content (18), said ticket (22) comprising at least, a time stamp (24), a counter (26) and a random number (28); a message authentication code attached to said ticket (22), which verifies the validity of the ticket at a provider of services (12) or content (18) when successfully decoded; and said counter (26) counting time periods in addition to said time stamp (24), thus making possible to differ between tickets (22) with time stamps (24) issued at a same time period.

13. A ticket according to claim 12, characterized in that a cost code field for requested services is added to said ticket.

14. A ticket according to claims 12-13, characterized in that said counter (26) is incremented at each access request, and reset at each current universal time coordinated (24) timestamp increment.

15. A ticket according to claims 12-14, characterized in that the ticket (22) is a long arbitrary number, represented as a linear sequence, a random sequence or a combination of both.
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 17/60
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic database consulted during the international search (name of database and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>WO 0109743 A1 (TB SOFT INC), 8 February 2001 (08.02.01)</td>
<td>1-15</td>
</tr>
<tr>
<td>A</td>
<td>US 5974309 A (FOTI, G.), 26 October 1999 (26.10.99)</td>
<td>1-15</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:
  "A" document defining the general state of the art which is not considered to be of particular relevance
  "E" earlier application or patent but published on or after the international filing date
  "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
  "O" document referring to an oral disclosure, use, exhibition or other means
  "P" document published prior to the international filing date but later than the priority date claimed
  "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
  "X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
  "Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
  "&" document member of the same patent family

Date of the actual completion of the international search: 17 December 2002

Date of mailing of the international search report: 18-12-2002

Name and mailing address of the ISA/Swedish Patent Office
Box 5055, S-102 42 STOCKHOLM
Facsimile No. +46 8 666 02 86

Authorized officer
Jan Silfverling/LR
Telephone No. +46 8 782 25 00
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>WO 0109743 A1</td>
<td>08/02/01</td>
<td>AU 3680600 A</td>
<td>19/02/01</td>
</tr>
<tr>
<td>US 5974309 A</td>
<td>26/10/99</td>
<td>AU 2796297 A</td>
<td>26/11/97</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BR 9708901 A</td>
<td>03/08/97</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 2000010681 A</td>
<td>25/02/00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 9742784 A</td>
<td>13/11/97</td>
</tr>
</tbody>
</table>