

ANONYMOUS ELECTRONIC TRANSACTIONSBACKGROUND

GSM originally stood for Groupe Spécial Mobile, a  
5 European study group formed in 1982 to study and develop  
criteria for a pan-European mobile telephone system. GSM is  
currently recognized as an acronym for Global System for  
Mobile communications, and represents the criteria developed  
as a result of the work of the Groupe Spécial Mobile. In  
10 general, GSM represents a set of mobile telephone standards  
and specifications. Equipment that meets GSM standards in  
one GSM network is compatible with any GSM network. GSM  
networks now exist worldwide.



15

DESCRIPTION OF DRAWINGS

\*159159\*

Figure 1 is a diagram of a communications network.

Figure 2 is a diagram of a communications network  
including an anonymizer.

Figure 3 is a conceptual diagram depicting the flow of  
20 data, and goods or services in an electronic transaction  
involving an anonymizer.

Figure 4 is a diagram of an anonymizer.

Figure 5 is a flowchart illustrating techniques for  
providing anonymizer service.



\*G00002\*

Figure 6 is a flowchart illustrating variable anonymity.

#### DETAILED DESCRIPTION

5       The techniques described below allow network subscribers to conduct electronic transactions with providers of goods and services, while maintaining a degree of personal privacy. The techniques are especially advantageous in the context of a GSM network, but are not  
10   limited to GSM.

GSM systems are digital systems that employ time division multiple access technology, allowing several subscribers to share a frequency channel at the same time. GSM systems are intended to interface with digital  
15   communication networks such as the Integrated Services Digital Network (ISDN). GSM systems are also intended to work with analog communication systems, such as the Public Switched Telephone Network (PSTN).

Figure 1 shows a typical communications network 10 that  
20   includes GSM systems. A subscriber obtains wireless access to network 10 via mobile device 12. Mobile device 12 may be any kind of terminal that accesses network 10, such as a mobile telephone handset. Mobile device 12 typically is assigned a unique International Mobile device Identity,  
25   which identifies each piece of mobile device 12 to network

10. In addition, mobile device 12' interfaces with  
Subscriber Identity Module (SIM) 14, which uniquely  
identifies the subscriber to network 10. A typical SIM 14  
is a smart card that is inserted into a GSM terminal. The  
5 subscriber can make and receive calls with mobile device 12.

Mobile device 12 accesses network 10 by establishing a  
wireless communication link with a base transceiver station  
16. Base transceiver station 16 includes a transceiver that  
defines a cellular calling area. Base transceiver station  
10 16 typically handles the wireless protocols with mobile  
device 12. A plurality of base station transceivers are  
generally managed by a base station controller 18. A  
plurality of base station controllers is usually coupled to  
a mobile services switching center 20, which typically acts  
15 as a central component in the cellular network. Base  
transceiver station 16, base station controller 18 and  
mobile services switching center 20 are typically operated  
under the auspices of a GSM provider 22.

Mobile services switching center 20 interfaces with  
20 other communication services, such as ISDN 24 and PSTN 30,  
each of which may be operated under the auspices of  
different communications suppliers 26, 28. ISDN 24 and PSTN  
30 provide service to subscribers such as telephone  
customers 32. In addition, ISDN 24 and PSTN 30 may each  
25 connect to automated subscribers 34, such as computers,

copying machines, toll booths or vending machines. Toll booths and vending machines, for example, may dispense services or goods when provided with a signal authorizing them to do so.

5        In typical network 10, a subscriber can use mobile device 12 to place an electronic order for goods or services. This transaction may be processed in several ways, such as by accessing an account or authorizing payment by credit card. One method for processing the transaction  
10 is to use subscriber data stored in SIM 14. Invoices can then be billed to the subscriber's account with GSM provider 22. Typically the entity receiving the order learns personal information from the subscriber's SIM 14 and mobile device 12, such as the subscriber's identity, location or  
15 calling pattern. In exchange for the simplicity of making an electronic transactional order for goods or services, subscribers may be giving up some of their privacy. The techniques described below allow GSM subscribers to preserve their privacy while making electronic transactional orders  
20 for goods and services.

Figure 2 shows a communications network 50 that includes a GSM system 52. Unlike network 10 of Figure 1, network 50 of Figure 2 includes an element 54 to be called herein an "anonymizer," because it provides anonymity  
25 service. In Figure 2, anonymizer 54 provides anonymity

service to GSM subscribers using network 50. Network 50 of Figure 2 also includes a payee 56, which may be an automated subscriber like automated subscriber 34 in Figure 1. A GSM user 58 who subscribes to the anonymity service provided by anonymizer 54 interfaces with network 50 via an interface such as mobile device 12. Payee 56 interfaces with network by way of an interface such as a connection to PSTN 30.

Anonymizer 54 is shown in Figure 2 as interposed between PSTN 30 and payee 56, but anonymizer 54 may communicate with payee 56 by way of PSTN 30, or by way of another communication channel. Furthermore, anonymizer 54 could be placed at other locations in network 50.

Anonymizer 54 could be, for example, part of GSM system 52 and operated under the auspices of GSM provider 22. Anonymizer 54 may alternatively be operated under the auspices of PSTN 30 or any other communication provider. The service of anonymizer 54 may also be offered by an anonymity service provider independent of the communication network. Furthermore, anonymizer 54 is not limited to application with an analog system such as PSTN 30, but may provide anonymity in a digital system such as ISDN 24 (not shown in Figure 2).

Subscriber 58 to the anonymity service provided by anonymizer 54 may conduct transactions by providing no personal data or by providing a selected amount of personal

data. Anonymizer 54 protects the privacy of subscriber 58 by providing no personal information, or limited personal information, to payee 56.

Figure 3 illustrates an exemplary transaction using anonymizer 54. Subscriber 58 places an electronic transactional order for a good or service from payee 56, using mobile device 12. Subscriber 58 sends information that will be needed to process the order, such as the kind of service desired or the quantity of product needed. In addition, other information about subscriber 58 may be transmitted automatically, such as the name of the subscriber, the location of the call and the equipment used to make the order. This information is passed to GSM system 52, and may be relayed via PSTN 30 to anonymizer 54.

Anonymizer 54 relays the order information to payee 56 (via PSTN 30 or other communication channel), but does not relay the other information about subscriber 58. Instead, anonymizer 54 may pass along limited information about subscriber 58. The information passed along is authorized by subscriber 58. For example, anonymizer 54 may pass along an address to which delivery is requested. In addition, payee 56 may pass information to anonymizer 54 to be relayed to subscriber 58, such as a confirmation number, or a demand for additional information. Anonymizer 54 may also pass along to payee 56 personal information about subscriber 58,

as will be described in more detail below. After receiving a satisfactory order, payee 56 provides the products or services to subscriber 58 or to a recipient designated by subscriber 58.

5        Payment for the products or services may be handled in several ways. As shown in Figure 3, a voucher may be passed to anonymizer 54, which relays an anonymizer voucher to payee 56. In general, a voucher represents an electronic payment authorization, such as a credit or other record  
10    exchangeable for payment. The voucher transmitted by anonymizer 54 to payee 56 may also represent a guarantee of payment, such that payee 56 does not bear a risk of nonpayment for products or services delivered.

Subscriber 58 ultimately pays for the goods or services  
15    provided by payee 56, but subscriber 58 typically pays an entity other than payee 56. For example, as illustrated in Figure 3, an arrangement between the GSM provider 22 and the anonymity service provider results in a voucher being transmitted from GSM system 52 to anonymizer 54. The bill  
20    for the goods or services may be added to the bill for GSM service sent to subscriber 58 by GSM provider 22. Alternatively, the bill for the goods or services is then to the bill sent to subscriber 58 by the anonymity service provider.

A system diagram of anonymizer 54 is shown in Figure 4. Anonymizer 54 includes communication interfaces 80 and 82, by which anonymizer 54 connects to PSTN 30 or ISDN 24, and by which anonymizer 54 communicates with subscriber 58 and payee 56. In some circumstances anonymizer 54 may function with a single communication interface. Anonymizer 54 also may include database 86, which stores information about subscribers, including directives as to the degree of anonymity desired by each subscriber.

10       Anonymizer 54 further includes processor 84, which performs several functions associated with anonymity service. For example, processor 84 retrieves information from database 86 about subscribers' desired anonymity. Processor 84 also receives subscribers' orders from one  
15       communication interface 80 and relays the orders via a second communication interface 82. In addition, processor 84 stores subscriber information in database 86. Anonymizer 54 may be implemented, for example, as a computer system. Techniques employed by anonymizer 54 may be implemented as  
20       software, which may be stored in a machine or computer system on any machine-readable medium such as a magnetic disk or optical drive, or may be stored within non-volatile memory such as read-only memory (ROM).

Figure 5 is a flowchart illustrating techniques for  
25       providing anonymizer service. In an exemplary

configuration, anonymizer 54 receives data related to a subscriber's order, such as the identity of the payee, the product or service desired, and the quality or quantity desired (90). Anonymizer 54 also receives data identifying the subscriber (90). Anonymizer 54 retrieves from its database information about the subscriber, including, for example, the degree of privacy to be afforded the subscriber.

Several degrees of privacy may be offered, providing a range of anonymity. One degree of anonymity is total anonymity. A payee receives no personal information about a subscriber having total anonymity. The subscriber may specify a lesser degree of anonymity by allowing anonymizer 54 to relay to payee 56, for example, information about the subscriber's name but not information about the subscriber's address, telephone number or calling patterns. The subscriber may also specify that information about him be kept from payee 56, but that demographic information about him be disclosed. A subscriber may permit payee 56 to know the town where subscriber lives, for example, without disclosing the subscriber's name or address. A subscriber may also provide payee 56 with a pseudonym or a frequent-purchaser identification code. Another form of anonymity may vary on the basis of the identity of the payee. The subscriber may authorize disclosure of more personal data

when ordering airplane tickets, for example, than when ordering flowers. A further form of anonymity involves "negotiated anonymity," which will be explained in more detail below.

5       After retrieving the information from the database (92), anonymizer 54 relays data to payee 56, such as the order and voucher information (94). Anonymizer 54 may also pass along to payee 56 anonymous identification data, i.e., data about the identity of the subscriber that the  
10   subscriber has authorized to be passed along. In addition, anonymizer 54 ordinarily processes the transaction (96), which may include debiting the subscriber's account for the voucher issued to payee 56, or acknowledging a voucher received from GSM provider 22. Anonymizer 54 may also relay  
15   information from payee 56 to the subscriber, such as a confirmation number (98).

      As described above, anonymizer 54 may provide a range of anonymity. Figure 6 is a flowchart illustrating a variable anonymity technique. In this technique, the degree  
20   of anonymity may become part of the transaction, and is automatically "negotiated" by anonymizer 54 on behalf of subscriber 58 and payee 56. Anonymizer 54 relays an anonymous order for a product or service to payee 56 (100), and includes an offer to provide additional information  
25   about subscriber 58 in exchange for consideration from payee

56, such as a discount. The offer is pre-authorized by subscriber 58. If payee 56 accepts (104), anonymizer 54 provides the additional information to payee 56 (110) and the transaction proceeds (112). Payee 56 may reject the offer and put forth a counteroffer (106). Payee's counteroffer may, for example, propose a smaller discount or request more information. Anonymizer 54 evaluates the counteroffer according to parameters previously authorized by subscriber 58, which are stored in database 86. If the counteroffer is not within the parameters, the counteroffer is rejected (114) and the transaction proceeds (112). If the counteroffer is accepted, anonymizer 54 provides the additional information to payee 56 (110) and the transaction proceeds (112).

The techniques shown in Figure 6 are for purposes of illustration. Variations of the techniques are possible. For example, payee 56 may initiate the offer to provide the product or service at a discount if additional information is provided, and anonymizer 54 may counteroffer. Subscriber 58 may also specify a range of permissible prices, quantities or degrees of personal information, allowing further offers and counteroffers. In addition, payee 56 may refuse to accept anonymous orders, in which case its counteroffer represents a stipulation that unless certain information is provided, there will be no transaction.

A number of embodiments of the invention have been described. Although the techniques for maintaining various degrees of anonymity have been described in the context of a GSM network, they may be adapted to any network in which a  
5 subscriber wishes to avoid having personal information passed to a payee. These and other embodiments are within the scope of the following claims.

CLAIMS

1. A method comprising:

receiving an electronic order from a first party;

receiving information about the first party;

5 transmitting the order to a second party;

transmitting less information about the first party to  
the second party than was received; and

transmitting a voucher to the second party.

2. The method of claim 1, further comprising transmitting

10 no information about the first party to the second party.

3. The method of claim 1, further comprising transmitting  
selected information about the first party to the second  
party, wherein transmission of the selected information is  
authorized by the first party.

15

15 4. The method of claim 1, further comprising retrieving  
information from a database concerning the first party, and  
selecting information about the first party for transmission  
to the second party based on the retrieved information.

5. The method of claim 4, wherein retrieving records from  
20 a database concerning the first party comprises retrieving

directives describing the information to be withheld from the second party.

6. The method of claim 1, wherein receiving information about the first party comprises receiving information about the first party from a subscriber identity module.

7. An article comprising a computer-readable medium which stores computer-executable instructions for receiving and transmitting information, the instructions causing a machine to:

receive an electronic transactional order from a first party;

receive information about the first party;

transmit the order to a second party;

transmit less information about the first party to the second party than was received; and  
transmit a voucher to the second party.

8. The article of claim 7, the instructions further causing the machine to transmit no information about the first party to the second party.

20

9. The article of claim 7, the instructions further causing the machine to transmit selected information about

the first party to the second party, wherein transmission of the selected information is authorized by the first party.

10. The article of claim 7, the instructions further causing the machine to retrieve information from a database  
5 concerning the first party, and select information about the first party for transmission to the second party based on the retrieved information.

11. The article of claim 10 wherein retrieving information from a database concerning the first party comprises  
10 retrieving directives describing the information to be withheld from the second party.

12. The article of claim 7 wherein receiving information about the first party comprises receiving information about the first party from a subscriber identity module.

15

15 13. A system comprising:

a processor and a database,  
wherein the processor is configured to receive  
information about a first party, wherein the processor is  
configured to receive an electronic transactional order from  
20 the first party, wherein the processor transmits the order  
to a second party, and wherein the database includes

information about the first party and directives describing the information about the first party to be transmitted to the second party.

14. The system of claim 13 further comprising a  
5 communication interface coupled to the processor.

15. The system of claim 14 wherein the processor receives information about the first party and an order from a first party by way of the communication interface.

16. The system of claim 14 wherein the processor transmits  
10 the order to a second party by way of the communication interface.

17. The system of claim 13 wherein the directives describing the information about the first party to be provided to the second party include parameters  
15 defining the information to be provided in exchange for consideration from the second party.

18. A system comprising:  
a communication network;  
a first party interface coupled to the network;  
20 a second party interface coupled to the network; and

an anonymizer, comprising a processor, a database and a communication interface, the anonymizer coupled to the network by the communication interface,

wherein the anonymizer receives information about a first party, the anonymizer receives an electronic order placed on the network through the first party interface, the anonymizer is configured to transmit the order to the second party interface, and the anonymizer is configured to transmit less information about the first party to the second party interface than was received.

19. The system of claim 18 wherein the communication network includes a GSM network.

20. The system of claim 19 wherein the first party interface includes a subscriber identity module, and wherein information about the first party received by the anonymizer is supplied by the subscriber identity module.

21. The system of claim 18 wherein the communication network includes an integrated services digital network.

22. The system of claim 18 wherein the communication network includes a public switched telephone network.

23. A method comprising:

placing an electronic order with a second party on  
behalf of a first party; and

providing information about the first party to the  
5 second party;

wherein the amount of information provided is a  
function of consideration from the second party.

24. The method of claim 23 further comprising offering to  
provide identifying information in exchange for  
10 consideration from the second party.

25. The method of claim 23 further comprising:

receiving an offer of consideration from the second  
party in exchange for providing information about the first  
party; and

15 deciding whether the offer is acceptable based upon  
parameters specified by the first party prior to placing the  
order.

26. An article comprising a computer-readable medium which  
stores computer-executable instructions for receiving and  
20 transmitting information, the instructions causing a machine  
to:

place an electronic order with a second party on behalf of a first party; and

provide information about the first party to the second party;

5        wherein the amount of information provided is a function of consideration from the second party.

27. The article of claim 26, the instructions further causing the machine to offer to provide identifying information in exchange for consideration from the second  
10 party.

28. The article of claim 26, the instructions further causing the machine to:

receive an offer of consideration from the second party in exchange for providing information about the first party;

15 and

decide whether the offer is acceptable based upon parameters specified by the first party prior to placing the order.