(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 August 2004 (19.08.2004)

PCT

(10) International Publication Number
WO 2004/070670 A1

(51) International Patent Classification[7]: G07F 7/10, G06F 1/00, H04L 29/06

(21) International Application Number: PCT/EP2004/050041

(22) International Filing Date: 23 January 2004 (23.01.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0301539.3 23 January 2003 (23.01.2003) GB

(71) Applicant *(for all designated States except US)*: **ATOS ORIGIN IT SERVICES UK LIMITED** [GB/GB]; South Quay Plaza II, 183 Marsh Wall, London E14 9SH (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **KOISTINEN, Martin** [GB/GB]; 3 Dorset Road, Windsor Berkshire SL4 3BA (GB).

(74) Agent: **WEIHS, Bruno**; Osha Novak & May, 121 avenue des Champs Elysées, F-75008 Paris (FR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.

(54) Title: PRIVACY ENHANCED SYSTEM AND METHOD COMPRISING FACT ASSERTION QUERY LANGUAGE

(57) Abstract: Privacy enhanced method for a customer to communicate personal data to an organization he has access to comprising the steps of. - receiving a request for personal information from a requesting entity belonging to said organization, such a request being presented into the form of an assertion admitting a response of the type "true" or "false"; - providing to the requesting entity the response of such an assertion, such a response being transferred with the control of the customer.

WO 2004/070670 A1

PRIVACY ENHANCED SYSTEM AND METHOD COMPRISING FACT ASSERTION QUERY LANGUAGE

The present invention is related to a privacy enhanced system and method comprising fact assertion query language.

Nowadays there is a constant development of transactions between organization and customer where customers are obliged to identify themselves and where personal data are collected. This can be the subject of considerable abuse.

For example, a customer who opens his purse or wallet, will find, somewhere in there, several forms of identification cards. Some of these were probably issued by some forms of authority such as government, employer or perhaps school.

It is likely that he also carries other "identification cards" from retailers in his area. These cards are often described as "loyalty cards" and he carries them because his retailer provides him with additional savings or points towards other benefits if he presents it every time he makes a purchase.

Some of the more successful loyalty card programs involve more than one retailer. For example, the card would be accepted, and earn benefits for him, at; his grocer, his favorite gasoline station, his favorite airline and perhaps a few of the specialty retailers that he frequents. For a consumer, this provides ample opportunity to amass greater savings or points towards the benefits the card offers.

However, loyalty card programs have really only one purpose – to collect and correlate information about customers; their spending habits, their brand preferences, their reaction to promotions, etc. This provides valuable marketing information for the retailers involved and, to a great extent; it helps them tailor their products and services to serve customers better.

Unfortunately, while the collection and analysis of such personal data by an organization (private or public) can be of great public benefit, it can also present some drawbacks in particular when links are made across organizations.

Privacy-aware consumers shy away from these programs – and for good reason. Armed with his personal details, any of the involved retailers could establish a match of a customer identity to credit agencies, public records, and more. Some of these retailers will also gain additional revenue by selling or renting customer personal details to other private organizations. Before too long, such a customer will find a tremendous amount of unsolicited offers in his mailbox and unsolicited salespeople calling he at suppertime. If he is an internet-enabled consumer, it won't be too long before his web browsing habits are also being collected against his profile and the content of spam and browser pop-up ads will start to reflect someone else's idea of who he really is.

Presented with these concerns, it is no wonder many people would object to any form of identification cards. Without the proper care, a ubiquitous identity card could compound the problem of widespread collection and correlation of the consumers personal details.

On the other side it is also beneficial for the public that each organization identifies their customers such for example for loyalty programs.

There is therefore a need that every organization had access to personal information for specific legal reasons, but also that personal information should not be disseminated.

The present invention solves the above problems by providing a system or a method, which allows every organization to verify some personal information of its customer but which prevent such organization to access without any control to all the personal information of the customer.

The present invention is based on the fact that the organization access mainly to truth value of assertions and that access to such information is controlled by the customer.

The invention will be further understood in connection with a detailed description of a practical example. Such an example is not limitative of the invention, which should have other forms of implementation.

Following the embodiment further described, each customer is provided with an identification card which allows him to access various organization (either public or private).

Such an identification card is equipped with an embedded cryptographic processor – a smart card. The cryptographic smart

chip was built from the ground up to securely hold information. It also provides a sufficient amount of computer processing and memory for the proposed innovations.

The identification card stores, among other things, public- and private keys. The cardholder will find these keys very useful in electronic transactions where he must prove his or her identity or electronically sign documents.

The card should be protected by the cardholder's personal identification number (PIN). This will allow a positive and culturally accepted means of approving operations on the card.

Some of the algorithms used to facilitate the functionality are already known. In particular, the application would use a cryptographic hash function at least in part.

Such an identification card store personal information on the customer such as his name, address and age. This card is to be presented for accessing various organizations (private or public), which need to access all or part of this personal information.

However in order to prevent from disseminating such a personal data, the card will not reveal the exact and full personal data but just mainly a response such as "true" or "false". Further, the cardholder will control all response to a query sent by a requesting entity by entering its PIN code.

For that the card and the requesting entity of the organization that ask for the personal data are equipped with an assertion application program.

The assertion application would allow specific assertions of fact to be made and their truth value returned. For example, a liquor retailer could require that the customer prove that he is of legal age to purchase alcohol. This application would allow a highly confident means of proving this assertion.

Since the application requires that the cardholder approve that the assert takes place, the cardholder is in full control of their details. Furthermore, the application does not allow for open-ended queries into the details of the cardholder. The facts are already known and exchanged by the parties. The fact is simply proven to a high degree of confidence by the application. Finally, the application only returns enough information to satisfy the legal requirements of those involved. In the case of the liquor store owner, he does not need to know the customer's current age or date of birth, just that he meets the legal requirements for buying alcohol.

Sometimes it is important for an organization to know certain facts about the cardholder before he or she can become a member of, or interact with the organization. For example, in order to by alcohol beverages from a retailer, the customer is typically asked to prove that he or she is of the legal age. The retailer doesn't need to know the customer's actual age, just that they are at least the minimum age. The author proposes another application on the card that can help.

Once the retailer verifies that the card is authentic and that the individual is the proper holder of that card, the retailer might ask the cardholder to insert his or her card into the trusted card-terminal for an age-verification. The cardholder would insert his or her card and the terminal would display the assertion that the retailer needs verified. If the local legal age for alcohol purchase were 21 and the current date were the 20th of January 2003, the terminal might read:

The cardholder is at least age [21] as of [20-Jan-2003]

The cardholder would then approve the assertion by entering the correct PIN for the card. The Assertion Applet would then decrypt the appropriate record on the card, compare the official date of birth for this cardholder to the date provided (20-Jan-2003), compute that it is at least the age provided and return simply true or false to the card-terminal, which would display the value for the retailer.

Note that this interaction does not reveal any more information about the cardholder than is necessary for retailer to fulfill their legal requirements. In fact, this sort of innovation would even allow the retailer to maintain receipts that each purchase of alcohol was to a legally aged customer.

The author proposes that the Assertion Application can interact with a number of data records on the card such as at least the cardholder's official name, official gender, official date of birth, official current residence.

Some example assertions might be:

To assert that the name the cardholder provided is their official name:

The cardholder's first name is [Martin].
The cardholder's Surname is [Koistinen].
The cardholder's full legal name is [Martin James Koistinen].

To assert that the cardholder is the proper gender to join a single-gender school:

The cardholder is [Male].

To assert that a cardholder is of legal age to enter a night club:

The cardholder is at least [21] years old as of [20-Jan-2003].

Verifying that a cardholder is eligible for a child-discount:

The cardholder is not yet [12] years old as of [20-Jan-2003].

To assert that the cardholder is a legal resident of a tax or voting district:

The cardholder is currently residing in the state of [England].
The cardholder is currently residing in the county of [Berkshire].
The cardholder is currently residing in the city of [Windsor].

Note that in each case, the single assertion is approved or denied. It would not be possible to simply ask for information about the

cardholder. First of all, the cardholder must approve the assertion first. Even then, if the assertion fails, no further information about the cardholder is revealed.

In general, the Assertion Application can be used to prove assertions that the cardholder declares of themselves. This means that the card only proves known facts. It does not reveal them. When a cardholder tries to buy alcohol, he or she is asserting that they are of the legal age. The application helps them prove it.

Since the card terminal can provide a receipt of the assertions and their answers, both parties have the ability to prove that only the right assertions were made, and that these were sufficient to allow or deny the membership or transaction. Imagine a case where a cardholder has gone to a job interview and the employer has asked to assert that he or she is at least the legal age to work, but the employer has instructed the card terminal to assert two facts:

The cardholder is at least age [15] as of [20-Jan-2003].
The cardholder is [male].

If it were inappropriate for the gender of the cardholder to be asserted for the position, the cardholder could firstly disallow the second assertion, then take a receipt of the assertion to the authorities as evidence of the employer's misconduct.

Additionally, the author proposes a variation of the application that would allow assertions to be made on certain emergency medical information. The application could be implemented so that with

proper authorization, emergency medical crews could make these assertions without requiring the possibly unconscious cardholder's PIN:

The cardholder is known to be allergic to [penicillin].
The cardholder is known to be a [hemophiliac].

Perhaps also with the proper authorization, more open-ended questions could be asked such as:

What is the cardholder's blood type?
What medications is the cardholder current prescribed to take?
What is the contact information for the cardholder's current doctor?

CLAIMS

1. Privacy enhanced method for a customer to communicate personal data to an organization he has access to, the method comprising the steps of:
receiving a request for personal information from a requesting entity belonging to said organization, the request being presented in the form of an assertion admitting a response of the type "true" or "false"; and
providing to the requesting entity a response to the assertion, the response being transferred with the control of the customer.

2. The method of claim 1, wherein said response is generated by a microprocessor embedded in a device belonging to said customer, said microprocessor calculating the truth value of the query based on customer personal data stored on the microprocessor.

3. The method of claim 2, wherein said response needs for being transferred to the requesting entity that the customer communicates a password to that device such as a PIN code.

4. A system to implement the method of claims 1 to 3, wherein said customer has a smart card to communicate with a terminal to the requesting entity, said smart card storing personal data and an algorithm to operate on the query transmitted by the terminal.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/050041

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10 G06F1/00 H04L29/06

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)
IPC 7 G07F G06F H04L

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2001/034840 A1 (LION STEPHANIE ET AL) 25 October 2001 (2001-10-25) claims 1,2; figures 3,5 paragraph '0021! - paragraph '0022! paragraph '0029! paragraph '0002! paragraph '0008! paragraph '0025!	1-4
X	FERREIRA R C: "THE SMART CARD: A HIGH SECURITY TOOL IN EDP" 1 September 1989 (1989-09-01), PHILIPS TELECOMMUNICATION REVIEW, PHILIPS TELECOMMUNICATIE INDUSTRIE N.V. HILVERSUM, NL, PAGE(S) 1-19 , XP000072642 page 1 - page 6	1,4

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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 document 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	Date of mailing of the international search report
25 June 2004	05/07/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kemény, M

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/050041

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 104 959 A (AT & T CORP) 6 June 2001 (2001-06-06) figures 1-6 column 6, line 3 - line 4 column 7, line 39 - line 54	1-4
A	DE 198 16 541 A (ORGA KARTENSYSTEME GMBH) 21 October 1999 (1999-10-21) column 1, line 7 - line 18	1-4
A	WO 99/46682 A (LINDLEY ROBYN ALICE ; CORDONNIER VINCENT MAXINE (FR)) 16 September 1999 (1999-09-16) page 9, line 16 - line 19	1-4
A	US 5 943 423 A (MUFTIC SEAD) 24 August 1999 (1999-08-24) column 10, line 1 - line 4	1-4
A	US 5 148 481 A (NECKYFAROW STEVEN W ET AL) 15 September 1992 (1992-09-15) column 4, line 11 - line 15	1-4
A	EP 0 421 409 A (IBM) 10 April 1991 (1991-04-10) page 4, line 9 - line 11	1-4
A	US 2002/194499 A1 (AUDEBERT YVES LOUIS GABRIEL ET AL) 19 December 2002 (2002-12-19) paragraph '0041!	1-4
A	US 5 745 571 A (ZUK EDWARD ANDREW) 28 April 1998 (1998-04-28) column 4, line 60 - line 65	1-4
A	EP 1 035 461 A (BDC EDV CONSULTING GMBH) 13 September 2000 (2000-09-13) paragraph '0009!	1-4
A	GB 2 346 239 A (IBM) 2 August 2000 (2000-08-02) page 5, line 19 - line 25	1-4

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/050041

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2001034840 A1	25-10-2001	FR 2780177 A1	24-12-1999
		CN 1304504 T	18-07-2001
		DE 69900851 D1	14-03-2002
		DE 69900851 T2	26-09-2002
		EP 1086415 A1	28-03-2001
		WO 9966388 A1	23-12-1999
EP 1104959 A	06-06-2001	US 5241599 A	31-08-1993
		EP 1104959 A2	06-06-2001
		AU 648433 B2	21-04-1994
		AU 2351392 A	08-04-1993
		CA 2076252 A1	03-04-1993
		DE 69232369 D1	14-03-2002
		DE 69232369 T2	23-01-2003
		EP 0535863 A2	07-04-1993
		JP 2599871 B2	16-04-1997
		JP 6169306 A	14-06-1994
		NO 923740 A	05-04-1993
DE 19816541 A	21-10-1999	DE 19816541 A1	21-10-1999
WO 9946682 A	16-09-1999	AU 2820999 A	27-09-1999
		WO 9946682 A1	16-09-1999
US 5943423 A	24-08-1999	NONE	
US 5148481 A	15-09-1992	US 5048085 A	10-09-1991
		CA 2026739 A1	07-04-1991
		EP 0421409 A2	10-04-1991
		JP 3237551 A	23-10-1991
EP 0421409 A	10-04-1991	US 5048085 A	10-09-1991
		CA 2026739 A1	07-04-1991
		EP 0421409 A2	10-04-1991
		JP 3237551 A	23-10-1991
		US 5148481 A	15-09-1992
US 2002194499 A1	19-12-2002	WO 02103979 A1	27-12-2002
		EP 1396136 A1	10-03-2004
US 5745571 A	28-04-1998	AT 207642 T	15-11-2001
		AU 671986 B2	19-09-1996
		AU 3818093 A	08-11-1993
		WO 9320538 A1	14-10-1993
		CA 2133200 A1	14-10-1993
		DE 69331006 D1	29-11-2001
		EP 0634038 A1	18-01-1995
		JP 7505270 T	08-06-1995
		SG 46692 A1	20-02-1998
EP 1035461 A	13-09-2000	AT 4805 U1	26-11-2001
		EP 1035461 A2	13-09-2000
GB 2346239 A	02-08-2000	JP 2000222362 A	11-08-2000
		KR 2000053495 A	25-08-2000
		TW 460819 B	21-10-2001