(12) UK Patent Application (19) GB (11) 2 397 676 (13) A

(43) Date of A Publication 28.07.2004

(21) Application No: 0301539.3

(22) Date of Filing: 23.01.2003

(71) Applicant(s):
ATOS ORIGIN IT SERVICES UK LIMITED
(Incorporated in the United Kingdom)
Southquay Plaza II, 183 Marsh Wall,
LONDON, E14 9SH, United Kingdom

(72) Inventor(s):
Martin Koistinen

(74) Agent and/or Address for Service:
Sensa
Gamma House, Enterprise Road,
Chilworth Science Park, SOUTHAMPTON,
Hampshire, SO16 7NS, United Kingdom

(51) INT CL^7:
G06F 17/60

(52) UK CL (Edition W):
G4H HTG

(56) Documents Cited:
EP 0864996 A2 EP 0810538 A2
PAJ English language abstract for JP 2168371 A
(Mitsubishi) 28.06.90

(58) Field of Search:
UK CL (Edition V) G4H
INT CL^7 G06F
Other: ONLINE: WPI, EPODOC, PAJ

(54) Abstract Title: **Privacy enhanced system using fact assertion language**

(57) 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.

In a preferred embodiment a customer presents a smart-card containing personal information to a card terminal which enquires as to whether the customer is at least 21 years old. The enquiry may be displayed. The cardholder then approves the assertion by entering a correct PIN to the card. A processor on the card decrypts the relevant personal file on the card and compares it to the request, to return either a true or false response.

GB 2 397 676 A

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1995

Original Printed on Recycled Paper

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 thc 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.

Application No:	GB 0301539.3	**Examiner:**	Russell Maurice
Claims searched:	all	**Date of search:**	30 June 2003

Patents Act 1977 : Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1	EP 0864996 A2 (HITACHI) see eg the abstract
A	-	EP 0810538 A2 (FUJITSU) see eg the abstract
A	-	PAJ English language abstract for JP 2168371 A (Mitsubishi) 28.06.90

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{V}:

G4H

Worldwide search of patent documents classified in the following areas of the IPC^{7}:

G06F

The following online and other databases have been used in the preparation of this search report:

WPI, EPODOC, PAJ