

AUTHENTICATION FACILITATOR METHOD

The present invention refers to an authentication method for use over a communication network, such as in particular the Internet, between a user and a service and/or product provider (collectively referred to as a service provider) using an authentication facilitator.

BACKGROUND OF THE INVENTION

10

Conventional authentication methods are strongly biased to the service providers, which allow the providers to validate their customers or users. However, the users are unable to tell whether they are dealing with a genuine or a fraudulent provider, and there is no easy or speedy way for the users to distinguish a genuine provider from a fraudulent one.

15

Examples of the current authentication methods are summarized below.

20

"User ID and Password" System

The most common means of authentication is the "User ID and Password" system. It is based on the idea that only the authorized user has the proprietary knowledge of one's own "password".

25

This is the most common authentication mechanism since the availability of online system in the 1950's. Despite its well-known limitations, the "User ID and Password" system still remains the primary way of authentication in the online world.

However, the "User ID and Password" system is subject to serious challenge if not administered properly for the users and the system administrators. User IDs and passwords may be leaked during generation, storage or intercepted during use. Easy to remember passwords are easy to guess while difficult to remember password are also difficult to administer. As the users need to access different computer systems, they tend to use easy to remember passwords for all systems or link them in a way that they can derive them easily. As a result, hacking is easy. For private networks, many user IDs and passwords are exposed in the clear form during logon.

For the Internet, many systems rely solely on transport level encryption such as Secure Socket Layer (SSL) to prevent interception of user IDs and passwords. Other variations use password hashing for enhanced security. However, the "User ID and Password" system is subject to fraudulent practice as it is possible to capture the complete user ID and password using a fraudulent web site and the hacker can then use them to sign on to a genuine web site of the service provider to produce harm to the

user and the service provider. One of the active hacking is the "man-in-the-middle" attack, a kind of interception and active hacking that naïve users may not easily be aware of the attack.

5

Public Key Infrastructure (PKI)

PKI access control systems use digital certificate technology and effectively the user digitally signs the transactions or activities. Digital signing of transactions is recognized by digital acts in many countries and administration as a legal proof of non-repudiation.

15 However, business applications of PKI based authentication are still in the infancy and they are typically not very user friendly and do demand the users to have some basic security knowledge for the system to be effective, e.g. certificate management. Without such security knowledge, it is still possible to falsify the web site with user interface that pretends to use the digital certificate though the hackers cannot create any meaningful transactions as it is infeasible to sign the transactions without the user's private key.

25

The future of PKI based authentication is promising once the issues of usability and falsification of service providers are solved.

Biometrics

The principle of biometrics authentication is based on
5 the matching of the physical (biological) characteristics
of the individual human body during a transaction against
a stored profile of the same individual that was enrolled
earlier.

10 Examples of biometrics include facial recognition,
fingerprint, palm print, hand and finger geometry, and
iris and voice recognition. Biometrics systems serve
different purposes in different domains of applications.
Some methodologies are more robust but costly and
15 difficult to implement while others are cheaper and easy
to use but less reliable.

Among other biometrics, fingerprint biometrics is well
accepted for its high accuracy in very low false
20 acceptance and false reject rates. However, fingerprint
biometrics authentication system is very costly and
difficult to implement and certain population of the
users may not have good fingerprints that can easily be
read by the biometrics system without compromising
25 accuracy.

A further complexity of biometrics authentication system
is the storage and transmission of biometrics templates.

A strong biometrics authentication system should eliminate or minimize the risks of leakage of biometrics secrets by using a sophisticated cryptographic process and on-the-spot comparison (typically onboard hardware
5 enabled comparison), meaning higher implementation costs. Otherwise, a compromised biometrics authentication system offers a false sense of security with multiple points of secret leakage.

10 *Multi-factor Authentication*

Multi-factor authentication systems employ more than one method of authentication to enhance the level of security. The multiple means of authentication would
15 complement each other's to create a stronger authentication mechanism. Typical examples include the use of biometrics or hardware token with the conventional "User ID and Password" system.

20 Using multiple authentication methods together may create a more secure system but it would lead to higher administration costs and usability challenges.

Technological advances in the last 30 years have resulted
25 in information systems becoming more and more sophisticated. Nowadays, information technology is a way of life that is so pervasive that it plays an indispensable part in our work and in our leisure

regardless of the computer literacy of the individual and the level of computerization of the organization. When the individual uses an automatic teller machine, one is using an advanced financial computer system and network
5 to conduct a transaction. Every retail purchase goes through some form of point of sales and backend processing system.

However, authentication systems are constantly under
10 attacks by sophisticated hackers with the objective to steal the embedded proprietary information value for non-financial transactions or monetary value for financial transactions. In the last decade, authentication means have evolved to address various types of attacks. Many
15 alternative means are mainly variations of the common "User ID and Password" system. The most robust means typically employ PKI or biometrics but they are likely to be difficult to use and expensive to implement and maintain. Other means use a combination of available
20 forms of authentication to provide two-factor or multi-factor authentication to minimize the chance of unauthorized access.

The purpose of user authentication is to distinguish a
25 genuine user from unauthorized ones such that the service/product provider may allow the user to perform certain activities with it. What is lacking or deficient is the opposite, i.e. service provider authentication to

enable the users to distinguish a genuine provider from fraudulent or fake ones.

In practice, the users can easily be misled by a fake web
5 site or computer system because what they see is just the
user interface and a fake web site can pretend to be the
genuine web site with a falsified authentication
dialogue. In this case, even the most robust
authentication mechanisms using hardware tokens or multi-
10 factor authentication would not distinguish such fake web
sites unless the user has some security knowledge and
spends the effort to double check every dialogue and
detail mechanism behind the basic user interface. There
is a demand for mutual authentication of the user and the
15 service provider.

For online transactions that involve an intermediary,
there is also a need for authentication of the
intermediary, which is important; as the two parties
20 concerned must be certain that they are dealing with a
genuine third party so as to rely on it.

The current authentication methods such as the "User ID
and Password" system, PKI and biometrics do not
25 facilitate the user to authenticate the service provider
and alleviate the risks of the "man-in-the-middle"
attack.

The subject invention seeks to mitigate or at least alleviate the aforesaid problems by providing an authentication facilitator method. The method facilitates a user to authenticate a service provider and alleviates
5 the risk of the potential "man-in-the-middle" attack.

SUMMARY OF THE INVENTION

According to the invention, there is provided an
10 authentication facilitator method for use over a communication network for a third party to facilitate a first party to authenticate a second party before conducting a transaction with the second party via the communication network, comprising the following steps:

- 15 (a) registering by the first party with the third party, including establishing a set of mutual authentication keys with the third party and defining a unique identification reference of the first party known to the first party and the third party;
- 20 (b) registering by the second party with the third party, including establishing a set of mutual authentication keys with the third party and defining a unique identification reference of the second party known to the second party and the third party;
- 25 (c) connecting by the first party to the second party and requesting a transaction with the second party;
- (d) sending by the second party an address of the third party to the first party;

(e) performing by the first party and the second party respective mutual authentications using the respective keys with the third party;

(f) generating by one of the first, second and third
5 parties a random code for use after success of the mutual authentications;

(g) sending by the third party the identification reference of the first party and the identification reference of the second party to the first party,
10 together with the random code if not yet known to the first party;

(h) sending by the third party to the second party the random code if not yet known to the second party;

(i) verifying visually by the first party the
15 identification references of the first party and the second party sent by the third party; and

(j) upon successful verification of the identification references, connecting by the first party to the second party with the random code for conducting said
20 transaction therewith, the random code being used for final verification by the second party based on the random code in hand.

Preferably, step (d) includes sending by the second party
25 a transaction address thereof to the first party, and step (j) includes connecting by the first party to the second party at the transaction address for conducting said transaction therewith.

It is preferred that step (f) comprises generating of the random code by the third party upon success of the mutual authentications.

5

Preferably, step (h) includes sending by the third party the identification reference of the first party to the second party.

10 More preferably, the authentication facilitator method includes after step (h) step (h') of identifying by the second party an account of the first party according to the identification reference of the first party received from the third party.

15

Further more preferably, step (h') includes subsequently accepting by the second party said transaction requested by the first party.

20 Yet further more preferably, step (h') further includes subsequently sending by the second party an acknowledgement to the third party.

Conveniently, the identification reference of the second
25 party comprises publicly known information.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will now be more particularly described, by way of example only, with reference to the accompanying drawings, in which:

5 Figure 1 is a schematic functional block diagram which depicts a network of three i.e. first, second and third parties and illustrates the initial operation of an embodiment of an authentication facilitator method in accordance with the invention involving the third party
10 for a transaction between the first party and the second party; and

Figure 2 is a schematic functional block diagram which illustrates the main operation of the authentication
15 facilitator method.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENT

Referring to the drawings, there are shown three parties
20 namely a user 100, a service provider (SP) 200 and an authentication facilitator (AF) 300 acting as a third party therebetween, connected together by a communication network 10 such as the Internet, for whom an authentication facilitator method embodying the invention
25 is to be performed online. In the majority of cases the user 100 uses a personal computer workstation or any other terminal such as an automatic teller machine, whereas the service provider 200 is represented by a

server-based website.

The user 100 may be an individual or corporate user, who is an existing or registered customer of the service provider 200 and preferably has opened an account with the provider 200, who may be a bank for example.

As illustrated in Figure 1, the user 100 and the service provider 200 must first register themselves with the authentication facilitator 300 in order to use the subject authentication method.

To establish mutual trust between the user 100 and the authentication facilitator 300, the user 100 sends a registration request to the authentication facilitator 300 (Box 1'). The authentication facilitator 300 and the user 100 will exchange a set of mutual authentication keys with each other (Box 2'). The authentication facilitator 300 will then generate a unique identification reference "1st_party_ID_Ref" to the user 100 (Box 3') for identifying the user 100, which is only known to both parties.

To establish mutual trust between the service provider 200 and the authentication facilitator 300, the service provider 200 sends a registration request to the authentication facilitator 300 (Box 4'). The authentication facilitator 300 and the service provider

200 will exchange a set of mutual authentication keys with each other (Box 5'). The service provider 200 will then send a unique identification reference "2nd_party_ID_Ref" for identifying itself to the authentication facilitator 300. This identification reference is preferably the name of the service provider 200 as publicly known or is at least readily recognizable as denoting the service provider 200, so that the user 100 can immediately understand.

10

The aforesaid initial setup is prerequisite, after which the user 100 and the service provider 200 may communicate with each other through the network 10 for an online transaction, such as a logon request or any other transaction after logon whether involving monetary value or not. The order in which the user 100 and service provider 200 register with the authentication facilitator 300 is immaterial.

20 In actual implementations, there will be many users 100 and many service providers 200 to use the authentication facilitator 300 according to the subject method. More than one authentication facilitator 300 is also anticipated.

25

As illustrated in Figure 2, the user 100 first initiates an Internet connection to the website of the service provider 200 and selects or requests a certain

service/transaction (Box 1) from/with the provider 200.
If the transaction requires authentication, the service
provider 200 will send to the user 100 the address of the
authentication facilitator 300 together with a specific
5 transaction address of its own for executing the
transaction (Box 2).

The user 100 will then perform mutual authentication with
the authentication facilitator 300 (Box 3) using the set
10 of mutual authentication keys as agreed during user
registration at the outset. Similarly, the service
provider 200 will also perform mutual authentication with
the authentication facilitator 300 (Box 4) using the set
of mutual authentication keys as agreed during the
15 aforesaid initial setup. The order of these mutual
authentications is irrelevant.

Upon successful mutual authentications between the user
100 and the authentication facilitator 300 and between
20 the service provider 200 and authentication facilitator
300, the authentication facilitator 300 will generate a
secret random code. The authentication facilitator 300
will then send the random code, the "1st_party_ID_Ref"
and the "2nd_party_ID_Ref" to the user 100 (Box 5), and
25 separately the random code and the "1st_party_ID_Ref" to
the service provider 200 (Box 6).

According to the "1st_party_ID_Ref" received from the authentication facilitator 300, the service provider 200 identifies and maps the user 100 to the user's account, if any, for processing the transaction request.

5

Upon meeting of all necessary criteria including for example genuineness of the user 100 and/or payment method, the service provider 200 may accept or consent to the transaction and then send an acknowledgement to the authentication facilitator 300 (Box 7).

10

Upon receipt of the acknowledgement, the authentication facilitator 300 will cause the workstation of the user 100 to display the "1st_party_ID_Ref" and the "2nd_party_ID_Ref" and request that the user 100 visually verifies the "1st_party_ID_Ref" and the "2nd_party_ID_Ref" (Box 8).

15

By visually checking the "1st_party_ID_Ref", the user 100 can feel (more) confident that the authentication facilitator 300 is genuine because only the genuine party has knowledge of its own identification reference as assigned during the initial setup procedure. This is a human assurance built or added upon the machine mutual authentication completed earlier on between the systems of the two parties 100 and 300.

20

25

By visually checking the "2nd_party_ID_Ref" - preferably

the common name of the service provider 200 - provided by the authentication facilitator 300 who is trusted, the user 100 can feel certain with whom it is about to deal with.

5

At this stage, both the user 100 and the service provider 200 are in the possession of the random code, that being a common secret code that has been generated and supplied by the authentication facilitator 300, who has been
10 authenticated by either party using the respective mutual authentication keys.

Upon successful visual verification of both of the identification references, the user 100 proceeds to
15 connect (or re-connect) to the service provider 200 at the transaction address provided by the service provider 200 for realizing the transaction, with the random code supplied by the authentication facilitator 300 (Box 9). The service provider 200 should compare the random code
20 now received from the user 100 with the one received earlier from the authentication facilitator 300 for confirmation or final verification before executing the transaction. Thus, if the two random codes do not match with each other, the service provider 300 will disconnect
25 the web session.

The subject authentication facilitator method allows the user 100 to verify the service provider 200 based on the

given "1st_party_ID_Ref" and "2nd_party_ID_Ref" as only the registered service provider 200 can invoke the correct display of the identification references.

5 The random code alleviates the "man-in-the-middle" attack as the random code is encrypted and sent through the network 10 from the user 100 to the service provider 200 so that the service provider 200 can verify the random code accordingly. In case of a "man-in-the-middle" attack, the service provider 200 will close the web session, as the random code cannot be passed to the proper web session correctly.

Given that the subject authentication facilitator method is concerned with authentication of the parties involved in preparation for an online transaction, specifics of the transaction are not important. Thus, the transaction may be executed at the same address of the service provider 200 as initially visited by the user 100. Also, the identification reference of the first party need not be supplied by the authentication facilitator 300 to the service provider 200 (for mapping the user 100 to its account) at the same time as the random code; it may be supplied at a later time.

25

It should be appreciated that the set of mutual authentication keys between the user 100 or service provider 200 and the authentication facilitator 300 can

be symmetric or asymmetric in nature. The user 100 may use a two-factor method where the mutual authentication keys are stored in key token protected by a personal identification number (PIN). The key token may be a
5 memory-based token or a hardware-based token. To approve the mutual authentication process, the user 100 may present the key token and enter the PIN. For the service provider 200, the set of mutual authentication keys is likely, but not absolutely required, to be stored in
10 tamper-resistant hardware security module to be controlled by the application software of the service provider 200.

Although the random code is preferably generated by the
15 authentication facilitator 300 as described, it may instead be created by one of the other two parties 100 and 200 so long as the random code can be securely shared by the user 100 and the service provider 200 without exposure to any parties other than the three parties
20 involved 100, 200 and 300. For example, the random code may be generated by the service provider 200 and supplied to the authentication facilitator 300 for use, i.e. forwarding to the user 100, upon successful mutual authentications between the user 100 and service provider
25 200 and the authentication facilitator 300. In this case, there should be no need for the authentication facilitator 300 to send the random code (back) to the service provider 200 because the provider 200 already

knows what the random code is.

For enhanced security, the communication between the user 100 and the service provider 200, between the user 100
5 and the authentication facilitator 300 and between the service provider 200 and the authentication facilitator 300 may be in an encrypted mode.

For privacy reasons, the authentication facilitator 300
10 may transform the original identification reference of the user 100 i.e. "1st_party_ID_Ref" using a one-way cryptographic key specific to each service provider 200 before sending to the specific service provider 200 such that it is not feasible to derive the original value of
15 the identification reference known only to the user 100 and authentication facilitator 300 and to infer the value of another transformation of the identification reference given to another service provider 200.

20 Furthermore, it is understood that retention of audit trail is optional and is unrelated to the operation of the subject authentication facilitator method. That is to say, the method does not rely on the retention of audit trail to operate.

25

The authentication facilitator method aims at facilitating the authentication between the user 100 and the service provider 200, and does not replace their

authentication roles. Accordingly, the service provider 200 should authenticate the user 100 using existing means such as the "User ID and Password" system or the digital signature method.

5

It is to be appreciated that if the digital signature method is used by the service provider 200 to authenticate the user 100, the service provider 200 should retrieve the public key of the user 100 to verify the digital signature of user 100. The public key is usually available in a digital certificate of the user 100 published in a public directory or obtained dynamically from the user 100 or a third party. The authenticity of the digital certificate can be verified with the public key of the Certificate Authority that issued the digital certificate and the validity of the digital certificate can be checked using the certificate revocation list (CRL) procedure or a real-time online certificate status protocol (OCSP) or other means.

20

The invention has been given by way of example only, and various other modifications and/or variations to the described embodiment may be made by persons skilled in the art without departing from the scope of the invention as specified in the accompanying claims.

25

CLAIMS

1. An authentication facilitator method for use over a communication network for a third party to facilitate a first party to authenticate a second party before conducting a transaction with the second party via the communication network, comprising the following steps:
 - (a) registering by the first party with the third party, including establishing a set of mutual authentication keys with the third party and defining a unique identification reference of the first party known to the first party and the third party;
 - (b) registering by the second party with the third party, including establishing a set of mutual authentication keys with the third party and defining a unique identification reference of the second party known to the second party and the third party;
 - (c) connecting by the first party to the second party and requesting a transaction with the second party;
 - (d) sending by the second party an address of the third party to the first party;
 - (e) performing by the first party and the second party respective mutual authentications using the respective keys with the third party;
 - (f) generating by one of the first, second and third parties a random code for use after success of the mutual authentications;

(g) sending by the third party the identification reference of the first party and the identification reference of the second party to the first party, together with the random code if not yet known to the
5 first party;

(h) sending by the third party to the second party the random code if not yet known to the second party;

(i) verifying visually by the first party the identification references of the first party and the
10 second party sent by the third party; and

(j) upon successful verification of the identification references, connecting by the first party to the second party with the random code for conducting said transaction therewith, the random code being used for
15 final verification by the second party based on the random code in hand.

2. The authentication facilitator method as claimed in claim 1, wherein step (d) includes sending by the second
20 party a transaction address thereof to the first party, and step (j) includes connecting by the first party to the second party at the transaction address for conducting said transaction therewith.

25 3. The authentication facilitator method as claimed in claim 1 or claim 2, wherein step (f) comprises generating of the random code by the third party upon success of the mutual authentications.

4. The authentication facilitator method as claimed in
any one of claims 1 to 3, wherein step (h) includes
sending by the third party the identification reference
5 of the first party to the second party.

5. The authentication facilitator method as claimed in
claim 4, including after step (h) step (h') of
identifying by the second party an account of the first
10 party according to the identification reference of the
first party received from the third party.

6. The authentication facilitator method as claimed in
claim 5, wherein step (h') includes subsequently
15 accepting by the second party said transaction requested
by the first party.

7. The authentication facilitator method as claimed in
claim 6, wherein step (h') further includes subsequently
20 sending by the second party an acknowledgement to the
third party.

8. The authentication facilitator method as claimed in
any one of claims 1 to 7, wherein the identification
25 reference of the second party comprises publicly known
information.