Abstract: The present invention is related to a method and system for authenticating sessions between mobile clients and a server in a network, wherein the server provides a plurality of services, wherein respective services require different levels of access security for any session to be activated between a respective mobile client requesting a session for a specific service and the server, wherein the access to the requested service will be limited if the mobile client has a capability of providing access security lower than required by the session to be activated.
AUTHENTICATION OF SESSIONS BETWEEN MOBILE CLIENTS AND A SERVER

The present invention is related to authenticating sessions between mobile clients and a server in a network, and especially to a method and system comprising a layering of access levels to services, wherein an access level provides a certain level of security for the session, and wherein a session is only granted if the mobile client has a capability to provide the level of access security required for the service being requested from the mobile client.

Modern telecommunication systems and mobile telephones provide a possibility to access a plurality of services regardless of where a person is located. This freedom of movement without missing any form of contact with other people and institutions and services is starting to become characteristics of our times. However, many types of services such as banking services may only be accessible over a network if the security of the session is high. There are many such schemes in prior art, and they work well if the client accessing the service do have the capability of providing the required level of security for the session. Mobile telephones are typically mobile clients having a limited computing power, memory capacity etc. which many times limits the practical use of a program running in the mobile telephone. Even though the mobile telephone may comprise a miniature computer system, the constraints on power consumption in the mobile telephone limits for example the functionality and processing speed of the mobile telephone. Therefore, a mobile telephone may typically not be of practical use if a session with a server requires a high degree of security, since the computational speed etc. would render the use too slow and frustrating for the user when security checks, encryption/decryption etc. is performed during the session. On the other hand, development of advanced mobile telephones continues and some models do have the capability to perform more complex routines, for example security related tasks.

However, not all aspects of services usually require the same level of security when being used. For example, with reference to a banking system, a balance statement does not require the same level of security when a user requests such a statement from his bank. When the user wants to transfer money, on the other hand, the security needs to be high. The prior art solution of such problems usually apply two different strategies. One strategy states that the security mechanism of access to sessions must follow the highest possible level of security anyhow, while another strategy is to deliver only services that do not require a high degree of security. The implication of the first strategy is that only a limited selection of mobile clients can be used, i.e. the mobile
clients that have a capability to provide the requested level of security. The second strategy implies that not all services will be accessible even though the mobile client does have a capability to provide the security level that is required by the service.

US 2007/00031 11 A! by Kiyotaka et. al. discloses a security system for mobile clients comprising biometric data. A user brings the mobile client or mobile telephone to a service area wherein an image of his biometric data is created. This results in a process wherein the mobile client functions as an individual card storing biometrics information being used in an authentication process. To perform such tasks the mobile client must have such capabilities which limits the selection of possible mobile clients.

US 2003/0004870 A1 by Johannes Janse Van Rensburg et. al. discloses a system wherein remote control of the mobile clients provides transfer between banking accounts being recorded in a database. The security is related to the fact that there is no direct access to accounts, which limits the functionality of the system.

US 2002678 A1 by Chow et. al. disclose a method for secure authenticatin of a first computer program to a second computer program. The method is based on a protocol comprising a one-time password calculation based on a seed value. This method allows a user to access different server computers providing different level of security level in each respective server computer.

According to an aspect of the present invention, services and not only the server-computer system as such may require different levels of access security, between them and/ or within each respective service. To access a service from a mobile client access is granted only if the mobile client can provide access security at a required level. That requires that the mobile terminal in itself has the necessary resources to provide the necessary security level. A mobile telephone may comprise a full blown computing environment while others do have limited memory, computing speed etc. that makes it impossible to execute for example an advanced encryption/decryption algorithm in the mobile terminal. Sometimes preinstalled security elements such as certificates must be present. If the service has different functionality, each functional aspect of the service may require a different level of security (for example certificate). For example, accessing an account from a mobile telephone has no security risks involved if the access is only to read out a balance statement of the account. Therefore, this type of service requires only a simple access control, for example the initial level of security is to enter a PIN code as part of the session. If the user also wants to transfer money from
an account to another, this part of the session would require a higher level of security, for example a one time password may be generated. Any mobile telephone can be used to enter a PIN code, but providing an embedded one time password calculator as part of the mobile telephone requires certain processing and functional capabilities of the mobile telephone. Therefore, access to this service would beneficially be provided if the server could identify the security capability of the mobile client accessing the server. If the mobile client for example does not provide one time passwords, the access of this mobile telephone is limited only to those services requiring for example a PIN code alone. In stead of providing a static limited access strategy, the teaching of the present invention allows an adaptation of access to services that is a function of the capabilities of the mobile client and the required level of security required by the respective services. When a service is accessed from a mobile terminal, the service must adapt what kind of functionality the service can allow to provide for the user of the mobile terminal according to spesific attributes, including physical attributes, of the mobile terminal itself.

According to an example of embodiment of the present invention, a method for authenticating an extent of interactions in a session between a user of a mobile terminal and a service in a server system is provided for by adapting a security level in the session that reflects the allowed extent of the interactions in the session based on the security level the mobile terminal is providing for in the session, by identifying the following:

a) identifying the user identity in the server,
b) identifying the mobile terminal identity,
c) identifying the mobile terminal security features, physical attributes of the mobile terminal and preinstalled security elements in the mobile terminal, and then,
d) evaluating the security level that can be provided for in the mobile terminal based on the identifications in step a), b) and c) and comparing this level of security with a required security level provided for by the service in the server that is required to be provided for in the session to be able to access all functionality of the service in the server, and then adapt the security level in the session according to the security level provided for by the mobile terminal, if the security level of the mobile terminal is less than the security level required by the service, then limit the extent of allowed interactions in the session to what is allowed at this lower security level.

According to another example of embodiment of the present invention a method for authenticating sessions between mobile clients and a server in a network is provided,
wherein the server provides a plurality of services, wherein respective services requires different levels of access security for any session to be activated between a respective mobile client requesting a session for a specific service and the server, wherein the access to the requested service will be limited if the mobile client has a capability of providing access security lower than required by the session to be activated, wherein the method comprises the steps of:

assigning a security level identifier to each respective service provided for in the server,

when the server receives a mobile client request for a service in the server, the server identifies the mobile client's capability to provide access security by either transferring an access security capability identifier from the mobile client to the server, or by using an identifier identifying the mobile clients identity and using the mobile clients identity to search a list of pre-recorded mobile clients in the server, wherein the list comprises records of the respective mobile clients access security capability identifiers,

in the server, comparing the service security level identifier with the mobile client access capability identifier, and whenever the mobile client capability identifier is compatible with the service security level identifier, authenticate the session between the mobile client and the server,

if the mobile client capability identifier is not compatible with the service security level identifier, then limit the access to the server from the mobile client.

According to another example of embodiment of the present invention, a respective service comprises a plurality of sub services, wherein each respective sub service requires a different level of access security, the method comprises a further step of assigning a security level identifier to the respective service comprising sub services having a description of the different access levels for each respective sub service.

According to another example of embodiment of the present invention, the authentication of a session between a mobile client and the server for a service further comprises a step of authenticating a user's identity, wherein the user is operating the mobile client.

According to another example of embodiment of the present invention, the step of authenticating a user's identity further comprises using an authentication mechanism
reflecting the level of access security provided for by the security level identifier assigned to the service the user is requesting.

According to another example of embodiment of the present invention, the authentication of a session between a mobile client and the server for a service further comprises a step providing authentication of the physical identity of the mobile client.

According to another example of embodiment of the present invention, the step of authenticating the mobile client's identity further comprises initializing a communication protocol in the server and the respective mobile client that is compatible with the session's required access security level.

According to another example of embodiment of the present invention, the communication protocol is one of a Secure Socket Layer (SSL) protocol, Transport Layer Security (TLS) protocol, Wireless Transport Layer Security (WTLS) protocol, Wireless Application Protocol (WAP), or similar protocol.

According to an example of embodiment of the present system, the method according to the present invention is implemented as a program being executed in a server computer in a network.

According to another example of embodiment of the present invention, a data carrier comprising program instructions is provided, wherein the instructions when downloaded to a mobile telephone enables the mobile telephone to have the access capability according to the present invention.

Figure 1 illustrates an example of client server configuration according to the present invention.

Figure 2 illustrates examples of steps for providing a client according to the present invention.

Figure 3 illustrates examples of steps for providing a client according to the present invention.

Figure 4 illustrates an example of downloading and activation of a client according to the present invention.
Figure 5 illustrates an example of sequence steps for authenticating a session according to the present invention.

Figure 1 illustrates an example of a typical use of an embodiment of the present invention. A mobile client, for example a mobile telephone, communicates with a server being a server system for a service provider, which for example can be a bank, insurance company or broker etc. Other application areas for a method and system according to the present invention can be mobile office systems, industrial automation systems, or any system that can benefit from having a layered access system for authenticating sessions between a client and a server. The layered structure of the access system according to the present invention allows any mobile client to be granted some form of access to services in a session with a security level adapted to the capability of the mobile client itself. Many types of services do actually have different needs for security related to the sessions between the client and the server. For example, a banking system may operate with a PIN code mechanism for securing access to some services while requiring a more elaborate security for other services, for example by requiring a one time password generated by a one time password calculator. An aspect of the present invention is the ability to always allow a certain level of access to a service from a mobile client, and not to reject completely the request for a session from the mobile client.

According to an example of embodiment of the present invention the plurality of services provided for in a server may each comprise a descriptor identifying the required security level each respective service need to have for being activated. This descriptor can be a link from a service entry point to a list or a database record, for example. According to yet another example of embodiment of the present invention, a service may have different security levels or sub services having different security access levels within the service itself. Such conditions can be accounted for in the descriptor as formatted sections, for example, wherein each respective section describes the relevant security level required for each respective sub service linked with this respective section. When a mobile client request a service, the capability of the mobile client to provide or participate in the session at a correct security level must be assessed by the server. According to an example of embodiment of the present invention, the mobile client may comprise a descriptor identifying the capability of the mobile client. Such a client capability identifier may be downloaded to the mobile client when a user registers himself as a user of services from the server provider's server, for example, hi
another example of embodiment of the present invention, the server may comprise a list of physical identities (telephone numbers, IP addresses etc.) or physical addresses of mobile clients in the network. Whenever a mobile client requests a service the client capability identifier is made available in the server, either via a transfer of the descriptor from the mobile client to the server, or by inquiring the list of mobile clients capabilities registered in the server. The server is then comparing the respective descriptors for the services and the requesting mobile client, and if the descriptors are compatible, the requested service is granted. If the descriptors are not compatible, the server may reject the request for the service completely, but preferably grant access at a predefined level, for example a security level only requiring a PIN code access mechanism for example, wherein any access from the mobile client to the server is correspondingly limited, for example only permitting reading information out of the server.

When a respective service has a layered access mechanism, wherein different functional elements of the service may require different levels of security to be executed, the security level identifier can for example comprise sections, wherein each respective sections is linked to respective functional elements of the services. When a mobile client requests a particular functional level for a service, the corresponding security level identifier section is compared with the mobile client capability identifier. The server is then comparing the respective descriptors for the services functional elements and the requesting mobile client, and if the descriptors are compatible, the requested functional element is granted. If the descriptors are not compatible, the server may reject the request for the functional element completely, but preferably grant access at a predefined level, for example providing a limitation of the functional element being requested, for example only permitting reading of information from the server.

As described in the example of embodiment of the present invention above, certain information elements regarding the respective descriptors must be initialized respectively in the server and in mobile clients wishing access to the server. In an example of embodiment of the present invention, a server operated by a service provider requires that users with mobile clients or mobile telephones register a user name and an identification of the mobile client, for example a telephone number in the server. Entry points in the server as known to a person skilled in the art can point to such information stored in the server. In an example of embodiment of the present invention, an identity of the mobile telephone, for example a telephone number, IP address etc. is read out from the mobile client. A list of mobile client identities, sorted according to the type of identity i.e. telephone number, IP address etc., is searched to identify if the client
capability identifier is registered locally in the server. If not, the client capability identifier is transferred from the mobile client. The descriptors are then compared as described above. This scheme also applies when there are descriptors related to sub services.

In the examples of embodiments of the present invention illustrated above, the mobile client capability identifier and security level identifier descriptors are outlined above as information elements comprising values or contents identifying a level of respectively a capability of physical attributes of the mobile client and security level required by services, which are initialized. However, it is within the scope of the present invention to extract this type of information through protocols, i.e., the server may obtain the value or information content of the mobile client capability identifier by interrogating the mobile client through an exchange of messages between the mobile client and the server, for example. Such exchange of messages is well known in the prior art. On the other hand, the mobile client can identify the value or information content of the security level identifier by exchanging messages with the server. It is therefore within the scope of the present invention that the mobile client assesses the level of security required by the session with a server, and that the mobile client only requests services that requires a security level that is compatible with its own level of providing security for the session.

As readily understood by a person skilled in the art, such an exchange of messages for establishing values or information contents of the descriptors according to the present invention may also be performed via a third participating system in the process. A security broker computer in a network can establish mobile client capabilities and security level requirements for services, and then inform parties about the conditions to the participating parties of a session that is to commence between a mobile client and a server. It is therefore within the scope of the present invention that grant of sessions according to the present invention can be performed outside the mobile client and/or server.

According to an example of embodiment of the present invention, a mobile client may acquire the correct initialization for utilizing services from a specific server as depicted in the flow diagram illustrated in figure 2. The method steps according to the present invention provides first a generic client configuration as depicted in figure 2, while a specific client may be produced according to the method steps illustrated in figure 3.
An aspect of the present invention is to provide a system authenticating a user according to actual requirements for authenticating a service. A simple user authentication scheme requires only user name and a password. Strong user authentication schemes require often that the user have possession of an item, for example a physical unit such as a one time password calculator or similar device. Such schemes also often require a "knowledge factor" known only to the user, for example a PIN code. According to an example of embodiment of the present invention, authentication of a user will not be performed if the service does not require a user authentication. It is also an aspect of the present invention to provide strong authentication without the needs for external items. It is further an aspect of the present invention to provide a secure communication channel independent of network providers.

With reference to figure 2, an example of a generic client generation is depicted. In this preferred embodiment of a method according to the present invention the first step is to identify which Java platform to use. The Java platform concept provides a network independent client which is one of the aspects described above of the present invention. Examples of Java platforms for mobile telephones are Mobile Information Device Profile (MIDP) and Connected Limited Device Configuration (CLDC) as known to a person skilled in the art. A next step is to select a secure communication platform. Examples of such platforms for mobile clients are: Secure Socket Layer (SSL), Transport Layer Security (TLS), Wireless Transport Layer Security (WTLS), Wireless Application Protocol (WAP), or similar protocol, as known to a person skilled in the art. Which one of the communication platforms that is selected is a function of the capabilities of the mobile client. A next step is to select a user authentication mechanism. Examples are enCap, BankID, or any similar type of authentication mechanism developed for mobile clients in a network. The type of authentication mechanism is a function of the capabilities of the mobile client. A further authentication mechanism can be installing a one time password calculator algorithm in the mobile client, for example such as a one time password algorithm that is part of the enCap solution. The use of this algorithm is dependent on the capabilities of the mobile client. If the authentication mechanism is a Java based solution the authentication mechanism is integrated before producing the generic platform. If the authentication mechanism is not Java based, an interface to the authentication mechanism is created before producing the generic platform.

With reference to figure 3, a specific mobile client is generated by selecting a specific service provider (or server(s)) together with the unique capabilities of the service
provider. A mobile client identity is then generated. In an example of embodiment of the present invention, a mobile client capability identifier can be part of this mobile client identity. The value or content of the mobile client capability identifier is related to the mobile client capability to execute algorithms, storage capacity etc. However, according to another aspect of the present invention, the client capability identifier can be used by the service provider to limit access to services of users using this particular mobile client despite the mobile client do have physical characteristics allowing a higher degree of security than reflected by the initialized mobile client capability identifier. This can for example be used to distinguish between super users, ordinary users etc. (user privileges) or reflect a status of a subscription of a particular service, for example. According to another example of embodiment of the present invention, the mobile client capability identifier can at any time be updated remotely from the server when communicating with the mobile client.

According to another example of embodiment of the present invention, a user performs following steps of a method according to the present invention comprising a Bank service provider:

- A user downloads a Java based mobile bank client and installs the client in his mobile telephone.
- A gateway of the system displays an activating code to the user on his mobile telephone display.
- The Java client reads out profile data from the mobile telephone.
- The user starts the Java client from the catalogue it was installed from if not starting automatically. This feature is dependent on the type of mobile telephone that is used.
- The Java client reads out profile data from the mobile telephone such that a user interface can be adapted to the mobile telephone display. Other features such a functional buttons are configured.
- The Java client identifies the communication capabilities of the mobile telephone and establishes a secure communication protocol.
- The Java client displays an activating page to the user.
- The user inputs the activating code.
- The user receives a starting page with a possibility to log into the server or activating services directly from the page.

These steps are illustrated in the sequence diagram depicted in figure 4. Figure 5 illustrates an example of a sequence diagram for authenticating a user according to the
present invention. Similar sequence diagrams can be provided for the authentication of a
physical identity of a mobile client, etc. as known to a person skilled in the art.

The method steps according to the present invention and a system providing
embodiments of method steps according to the present invention is applicable in any
client server configuration in a network, wherein the client can be a physical entity (a
mobile telephone for example) or a logical entity (a software entity), wherein it is
beneficial to provide a layered security access scheme from clients to services provided
for in the server. Examples of such areas can be a banking server system, a broker
server system, an insurance server system, a mobile office system, an industrial
automation server system, or similar type of server system.
**Claims:**

1. A method for authenticating an extent of interactions in a session between a user of a mobile terminal and a service in a server system by adapting a security level in the session that reflects the allowed extent of the interactions in the session based on the security level the mobile terminal is providing for in the session, wherein the method comprises:

   a) identifying the user identity in the server,
   b) identifying the mobile terminal identity,
   c) identifying the mobile terminal security features, physical attributes of the mobile terminal and preinstalled security elements in the mobile terminal,
   d) evaluating the security level that can be provided for in the mobile terminal based on the identifications in step a), b) and c) and comparing this level of security with a required security level provided for by the service in the server that is required to be provided for in the session to be able to access all functionality of the service in the server, and then adapt the security level in the session according to the security level provided for by the mobile terminal, if the security level of the mobile terminal is less than the security level required by the service, then limit the extent of allowed interactions in the session to what is allowed at this lower security level.

2. The method according to claim 1, wherein the required security level provided for by a service is registered in the server computer as an access security descriptor linked to the service, and the security level that can be provided for by the mobile terminal as a mobile client capability identifier descriptor, wherein the the mobile client capability identifier is prestored in the mobile terminal, or is stored in the server linked to the respective stored mobile terminal identifier.

3. The method according to claim 1, wherein a respective service comprises a plurality of sub services, wherein each respective service and corresponding sub services of this service requires a different level of access security, the method comprises a further step of assigning a security level identifier to the respective service comprising sub services having a description of the different access levels for each respective sub service.
4. The method according to claim 1, wherein the step of authenticating the mobile client's physical identity further comprises initializing a communication protocol in the server and the respective mobile client that is compatible with the session's required access security level.

5. The method according to claim 4, wherein the communication protocol is one of a Secure Socket Layer (SSL) protocol, Transport Layer Security (TLS) protocol, Wireless Transport Layer Security (WTLS) protocol, Wireless Application Protocol (WAP), or similar protocol.

6. The method according to any previous claim, wherein the mobile client capability identifier is set according to user privileges, or a status of a user account on the server system.

7. The method according to any previous claim, wherein the mobile client capability identifier is updated in the mobile client remotely from the server.

8. The method according to any previous claim, wherein a value or information content of the mobile client capability identifier and/or security level identifier respectively is obtained through an exchange of information between the mobile client and the server.

9. The method according to any previous claim, wherein a value or information content of the mobile client capability identifier and/or security level identifier is obtained through an initialization of the respective mobile client capability identifier and the respective security level identifier parameter.

10. The method according to claim 8, wherein a third participating system in the network is obtaining a value or information content of the mobile client capability identifier and/or security level identifier respectively through an exchange of information between the
third participating system and mobile client, and between the third participating system and the server.

11. The method according to claim 2 and 8, wherein a step of comparing the mobile client capability identifier and the security level identifier is performed in the mobile client, and wherein a mobile client will limit requests for services only for services that has a security level identifier compatible with the mobile client capability identifier.

12. A server system in a network for authenticating sessions between mobile clients and the server in the network, wherein a program executed in the system is arranged to perform steps of the method according to claim 1 to 11.

13. The system according to claim 12, wherein the server system is one of a banking server system, a broker server system, an insurance server system, a mobile office system, an industrial automation server system, or similar type of server system.

14. The system according to claim 12, wherein a specific level of access security is provided for by entering a PIN number via the mobile client, while another of the different levels of access securities is provided for by generating and entering a one time password via the mobile client.

15. The system according to claim 12, wherein the mobile client is a mobile telephone, wherein the mobile telephone can provide access security capability to sessions with the server after being initialized by a service provider providing the plurality of services in the server, wherein the initialization comprises downloading an authentication mechanism that is a function of the capabilities of the specific mobile client's functionality.

16. The system according to any claim 12 to 15, wherein the mobile client comprises a Mobile Information Device Profile (MIDP) and a Connected Limited Device Configuration (CLDC).
17. The system according to any claim 12 to 15, wherein the mobile client comprises a one-time password generator device.

18. A data carrier comprising program instructions, wherein the instructions when loaded into a mobile client enables the mobile telephone to have the access capability according to claim 13.
Fig. 1
Production of generic client

1. Select Java platform
2. Select platform for secure communication
3. Select authentication solution
4. Java based?
   - Yes: Integrate authentication client
   - No: Integrate interface to authentication client
5. Produce generic client

Fig. 2
Production of customize...

Select Service Provider

Include Service Provider's unique capabilities

Produce a unique client ID

Fig. 3
INTERNATIONAL SEARCH REPORT

International application No
PCT/NO2009/000172

A CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
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: H04L

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 data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

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>X</td>
<td>US 20020169874 Al (BATSON ET AL), 14 November 2002 (14.11.2002), figures 3,4A,4B,4C, claims 1-20, abstract, paragraphs (0003)-(0007),(0015)-(0035)</td>
<td>1-18</td>
</tr>
<tr>
<td>A</td>
<td>US 20030030680 Al (COFTA ET AL), 13 February 2003 (13.02.2003), abstract, paragraphs (0022)-(0027)</td>
<td>1-18</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Special categories of cited documents:</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>document defining the general state of the art which is not considered to be of particular relevance</td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>earlier application or patent but published on or after the international filing date</td>
<td></td>
</tr>
<tr>
<td>L</td>
<td>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 (as specified)</td>
<td></td>
</tr>
<tr>
<td>O</td>
<td>document referring to an oral disclosure, use, exhibition or other means</td>
<td></td>
</tr>
<tr>
<td>P</td>
<td>document published prior to the international filing date but later than the priority date claimed</td>
<td></td>
</tr>
</tbody>
</table>

Date of the actual completion of the international search: 13 July 2009

Date of mailing of the international search report: 14 -07- 2009

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

Authorized officer
Hassan Khatoun Neama / JA A
Telephone No. + 46 S 782 25 00

Form PCT/ISA/210 (second sheet) (July 2008)
<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>US 20070101418 A1 (WOOD ET AL), 3 May 2007 (03.05.2007), abstract, paragraphs (0003)-(0009), (0030)-(0034)</td>
<td>1-18</td>
</tr>
</tbody>
</table>
International patent classification (IPC)

H04L 29/06 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded:
• From "Cited documents" found under our online services at www.prv.se (English version)
• From "Anforda dokument" found under "e-tjanster" at www.prv.se (Swedish version)
Use the application number as username. The password is VDGWIFGCZF.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.
<table>
<thead>
<tr>
<th>Patent Number</th>
<th>Type</th>
<th>Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>US 2002169874</td>
<td>A1</td>
<td>14/11/2002</td>
<td>NONE</td>
</tr>
<tr>
<td>US 20030030680</td>
<td>A1</td>
<td>13/02/2003</td>
<td>NONE</td>
</tr>
<tr>
<td>US 20070101418</td>
<td>A1</td>
<td>03/05/2007</td>
<td>NONE</td>
</tr>
</tbody>
</table>

Form PCT/ISA/2 10 (patent family annex) (April 2005)