BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS	**BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE**	**CHAMBRES DE RECOURS DE L'OFFICE EUROPÉEN DES BREVETS**

Internal distribution code:
(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 29 January 2014

Case Number:	T 2145/09 - 3.5.06
Application Number:	02737518.7
Publication Number:	1436682
IPC:	G06F1/00
Language of the proceedings:	EN

Title of invention:
SYSTEM AND METHOD FOR SPECIFYING SECURITY, PRIVACY, AND ACCESS CONTROL TO INFORMATION USED BY OTHERS

Applicant:
LINK US ALL, LLC

Headword:
Specifying security, privacy and access control/LINK US ALL

Relevant legal provisions:
EPC Art. 54(1), 84, 111(1)
EPC R. 29(2)

Keyword:
Novelty - (yes)
Claims - conciseness (yes)
Remittal to the department of first instance - (yes)

Decisions cited:

Catchword:

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 2145/09 - 3.5.06

DECISION
of Technical Board of Appeal 3.5.06
of 29 January 2014

Appellant:
(Applicant)

LINK US ALL, LLC
8F4272 Dant Boulevard
Reno, NV 89509 (US)

Representative:

Ahner, Philippe
BREVALEX
95 rue d'Amsterdam
75378 Paris Cedex 8 (FR)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted on 22 June 2009 refusing European patent application No. 02737518.7 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman:	D. Rees
Members:	A. Teale
	W. Sekretaruk

Summary of Facts and Submissions

I. In a communication dated 3 December 2003 relating to the results of a partial international search, the EPO as International Searching Authority invited the applicant to pay an additional search fee on the basis that International patent application No. PCT/US02/19100, which subsequently led to European patent application No. EP 02 737 518.7, claimed two groups of inventions. The first group were set out in claims 1 to 7, 31, 36 and 41, and the second group were set out in the remaining claims, namely 8 to 30, 32 to 35, 37 to 40 and 42. The application was found to lack unity, Rules 13.1 and 13.2 PCT, on the basis that the common concept linking claim 1 and those of the second group lacked novelty in view of the disclosure of the following document:

D1: Ashley P., Vandenwauver M. and Claessens J., "Using SESAME to Secure Web Based Applications on an Intranet", Secure Information Networks, Proceedings of the IFIP TC6/TC11, Joint Working Conference on Communications and Multimedia Security, CMS'99, 20 to 21 September 1999, Leuven, Belgium, pages 303 to 317, XP002260869.

II. No further search fees were paid by the applicant, and the International Search Report states that the search only relates to original claims 1 to 7, 31, 36 and 41.

III. The appeal is against the decision, dispatched on 22 June 2009, by the examining division to refuse the above European patent application on the basis that the subject-matter of claim 1 according to the then main request lacked novelty and inventive step, Articles 54(1,2) and 56 EPC 1973, in view of D1 and that the subject-matter of claim 1 according to the then auxiliary request lacked inventive step, Article 56 EPC 1973, in view of D1.

IV. A notice of appeal was received on 13 August 2009 in which the appellant requested that the appealed decision be set aside and a patent granted. The appeal fee was paid on the same day.

V. With a statement of grounds of appeal, received on 26 October 2009, the appellant filed amended claims according to a main and an auxiliary request as basis for the appeal and made an auxiliary request for oral proceedings should the board envisage confirming the refusal of the application.

VI. The application documents on file are consequently as follows.

Description (main and auxiliary requests):
Pages 1 to 18, as published on 27 December 2002 as WO 02/103499 A2.

Claims:
Main request: 1 to 36, received on 26 October 2009.
Auxiliary request: 1 to 24, received on 26 October 2009.

Drawings (main and auxiliary requests):
Pages 1/11 to 11/11 as published on 27 December 2002 as WO 02/103499 A2.

VII. The independent apparatus claims according to the main request read as follows:

"29. An apparatus for issuing an electronic document comprising: means for establishing a grantor certified reference, a requestor certified reference, and access control rules for said requestor; and means for incorporating said grantor certified reference, said requestor certified reference, and said access control rules in the electronic document digitally signed by said grantor, wherein said grantor grants access to information stored in a computer system owned by a third party to said requestor."

"30. An apparatus for accessing information comprising: means for receiving an electronic document digitally signed by a grantor, said electronic document having a grantor certified reference, a requestor certified reference, and access control rules for said requestor; and means for appending a digitally signed request for access to the information to said electronic document by said requestor, wherein said grantor grants access to information stored in a computer system owned by a third party to said requestor."

"31. An apparatus for validating access to information comprising: means for receiving a request digitally signed by a requestor, said digitally signed request having an electronic document digitally signed by a grantor, said electronic document having a grantor certified reference, a requestor certified reference, access control rules for said requestor; and means for validating said request using said requestor certified reference and said access control rules for said requestor, wherein said grantor grants access to information stored in a computer system owned by a third party to said requestor."

There are three each of corresponding independent method and "program storage device" claims. In addition there is a single independent claim to:

"35. An electronic document comprising: a grantor certified reference; a requestor certified reference; at least one access rule; and a grantor digital signature coupled to said grantor certified reference, said requestor certified reference and said at least one access rule, wherein said grantor grants access to information stored in a computer system owned by a third party to said requestor."

VIII. In view of the board's decision the wording of the claims according to the auxiliary request is immaterial.

Reasons for the Decision

1. The admissibility of the appeal

In view of the facts set out at points III to V above, the appeal fulfils the admissibility criteria under the EPC and is consequently admissible.

2. The context of the invention

2.1 The application relates to delegating access rights in the form of a "mandate" to information. For instance, a user can securely delegate part of its authority to a "financial portal" which acts as a proxy to aggregate financial information about the user from a variety of sources. Since the sources of information can distinguish proxy access from user access, the user need not rely on the good behaviour or internal security of the aggregator. According to paragraph [0008], access to user information can depend on "context", for example geographical location, time and device type.

2.2 Prior to issuance of a mandate, the issuer (also termed the "target person" in the description and the "grantor" in the claims) generates a private/public key pair and obtains a public key certificate from the holder of the resources which are to be accessed (termed a "third party" in paragraph [0016] and "service provider" in paragraph [0021]), a public key certificate binding the public key to the issuer. Further, a beneficiary (termed the "requester" in the claims) sends a "beneficiary certified reference" to the issuer (see paragraph [0029]). The issuer produces an "electronic document" (see figure 3), usually referred to in the application as a "mandate", allowing the beneficiary to access specified information sources and containing an issuer certified reference, the beneficiary certified reference, a date of issuance and access control rules for the beneficiary. The integrity of the electronic document is ensured by a digital signature mechanism (paragraph [0032]). The electronic document can comprise digital signatures conforming to the ITU X.509 standard (see below). The electronic document is then sent to the beneficiary.

2.3 As shown in figure 4, the electronic document or mandate is created in a sequence of transactions between the issuer and the beneficiary via a "mandate authority" which is part of the apparatus holding the resources (see figure 2 and paragraphs [0037] to [0040], where B is the issuer and A the beneficiary).

2.4 To request access to information on behalf of the issuer the beneficiary sends a signed request (see figure 6 and paragraph [0045]) including the mandate to a service provider. As shown in figure 7, the service provider only grants the requestor access to the issuer's information if the issuer, beneficiary and request are all valid.

3. The use of ten independent claims

3.1 According to the "Additional comments" section of the appealed decision, the main and auxiliary requests then on file did not fulfill the requirements of Article 84 EPC in combination with Rule 43(2) EPC, since they contained excessive independent claims in a particular category.

3.2 Regarding the requests now on file, the appellant has argued that the claims according to the main request meet the requirement of Rule 43(2) in combination with Article 84 EPC, since claims 1, 29 and 32 are respectively directed to a method, an apparatus and a computer readable storage device for issuing an electronic document, claims 8, 30 and 33 are respectively directed to a method, an apparatus, a computer readable storage device for requesting access to an information by using this electronic mandate and claims 18, 31 and 34 are respectively directed to a method, an apparatus, and a computer readable storage device for validating access to an information on the basis of a received request and an electronic mandate. Finally claim 35 sets out the electronic document itself. The independent claims thus concern interrelated methods, apparatuses and computer storage media and therefore fall within the exception provided in Rule 43(2)(a) EPC.

3.3 Since the application was filed on 14 June 2002 and was thus pending on the date of entry into force of EPC 2000 on 13 December 2007, the board understands the references in the decision and the statement of grounds of appeal to Article 84 and Rule 43(2) EPC as being to Article 84 and Rule 29(2) EPC 1973, respectively.

3.4 The text of Rule 29(2) EPC 1973 applicable to the present application is that amended by the decision of the administrative council of 13 December 2001 (see OJ EPO 2002, page 2). According to Article 2 of that decision, the amended text of Rule 29(2) EPC 1973 applied to all European patent applications, such as the present one, in respect of which a communication under Rule 51(4) EPC 1973 had not yet been dispatched.

3.5 According to Rule 29(2) EPC 1973 as so amended, a European patent application may contain more than one independent claim in the same category (product, process, apparatus or use) only if the subject-matter of the application involves one of the following:

(a) a plurality of interrelated products;

(b) different uses of a product or apparatus;

(c) alternative solutions to a particular problem, where it is not appropriate to cover these alternatives by a single claim.

3.6 Of the claim categories set out in the Rule, the board considers that the electronic document disclosed in the application can be most readily categorized as an "product", since it is generated by the apparatuses issuer, beneficiary and "mandate authority" and has a static existence e.g. in the memory of the beneficiary. This product plays a role in the operation of plural apparatuses which issue the electronic document, access information by generating a request including the electronic document and validate access to information by receiving a request including the electronic document The subject-matter of claims 29, 30 and 31 can consequently be seen as a plurality of interrelated apparatuses. Thus the board finds that condition "a" (a plurality of interrelated products) is fulfilled, albeit by apparatuses rather than by products (following T 0056/01, T0067/06 and T 1232/07). It follows that the European patent application may contain more than one independent claim in the same category. It is commonplace that an independent claim in one category may be accompanied by corresponding claims in other categories, where appropriate.

3.7 Consequently, as argued by the appellant, the claims according to the main request fulfil Rule 29(2) EPC 1973 as amended and Article 84 EPC 1973 regarding the conciseness of the claims.

4. Document D1

4.1 As explained below, D1 is less relevant to the claimed subject-matter than was found in the appealed decision.

4.2 D1 does not mention the delegation of information access rights by a grantor (issuer) to a requestor (beneficiary). Instead D1 concerns overcoming what are seen as the limitations of TLS (Transport Layer Security, successor to Secure Sockets Layer (SSL)) to provide access control for web based applications in organisational intranets by using the SESAME (A Secure European System for Applications in a Multi-vendor

Environment) security architecture instead; see abstract. Although SESAME uses the same GSS-API interface as TLS and thus is a suitable replacement, existing web servers and browsers do not provide hooks for replacing TLS. Two alternative solutions to this problem are proposed: firstly, extending TLS to carry attribute certificates and, secondly, a hybrid TLS/ SESAME solution. As stated on page 304 regarding the second alternative, "Our solution involves the integration of TLS and SESAME V4: SESAME V4 is used for user authentication, non-repudiation, access control and auditing, and TLS is used for end to end security in the traditional way".

4.3 According to Section 2, SESAME and TLS both offer security services to client-server systems. Although they can be used separately, a combination offers more flexibility. As table 1 on page 305 shows, SESAME not only offers all the services offered by TLS but also those of access control, non-repudiation of origin and auditing. SESAME and TLS differ in that SESAME is a security architecture, and is therefore situated in the application layer at the top of the TCP/IP reference model, whilst TLS is a standard defining the securing of communication between two parties and thus is situated a layer below SESAME in the transport layer. This difference influences the kind of services that they respectively provide, i.e. they are not in detail the same.

4.4 Both TLS and SESAME offer user authentification. In the case of SESAME, users can log on to a network once, receive a SESAME access token termed a "PAC" (Privilege Attribute Certificate), and use this token to access all resources on the network; see page 305, last paragraph. In contrast, since TLS is situated in the transport layer, TLS authenticates the client workstation rather than the user.

4.5 The security service of access control, offered by SESAME but not by TLS, relates to how a web server can know the privileges enjoyed by an authenticated user. Section 4 relates to extending TLS to provide access control by using ideas from the SESAME PAC structure to integrate TLS and SESAME so that TLS can transport SESAME PACs. A server can thus obtain a client's privileges by receiving an AC (Attribute Certificate). The server can also verify the integrity of the AC. The AC is a structure based on X.509, table 2 listing the AC fields. These include the issuer (the entity who produced and signed the AC), the owner (the entity with whom the attributes are associated), the attributes themselves and the signature (containing the digital signature of the AC issuer). The AC also contains access control information such as group membership, role information and clearance information. According to figure 1 on page 309, a server can either acquire an AC from the AC issuer (termed "Server acquisition") or look up an AC in a directory (termed "Server Lookup"). Alternatively, a client can acquire an AC from an AC issuer (termed "Client Acquisition") and send it to the server (termed "AC Push"). In these transactions TLS is used to establish connections between the client, AC issuer and server.

4.6 Section 5 relates to the integration of SESAME and TLS to overcome the problems that no implementation of TLS is available for the scheme in section 4 and that, according to this scheme, decisions such as who gets access to what are being taken at a level transparent to the end user. In this scheme both SESAME and TLS are provided, and TLS is not extended, in contrast to the scheme of section 4. The hybrid solution brings web-based applications under the umbrella of SESAME and, since it uses Java, does not require changes to users' browsers. The solution also allows users with smart cards to work on any workstation on the intranet. According to the hybrid solution, SESAME allows a user to obtain a PAC, and TLS is used to prove who is the owner of the PAC. TLS also provides entity authentication, data confidentiality and data authentication. SESAME proves access control, non-repudiation of origin and auditing; see table 4 on page 311.

4.7 Section 5.2 outlines how a user can sign in to SESAME and access system resources. In a first step, the user's client contacts the SESAME web server via a connection secured by TLS and downloads a login applet. In the second step, the applet performs the SESAME login protocol, during which the client provides the user's name and X.509 certificate. If authentification is successful then the client receives a PAC containing the user's privileges (role) and the unique identifier of the X.509 certificate (XID) used to authenticate the user. The PAC is valid for a limited period of time and is digitally signed by the issuer. In a third step, the PAC is stored as a cookie on the user's system so that it can be sent to any application server to provide credentials. In a fourth step, RBAC (role-based access control) is performed. When the user's client sends a request by a TLS-secured connection to an application server it also sends its cookie (PAC). A CGI (common gate interface) program verifies whether the PAC is valid and whether the user is the legitimate owner of the PAC. The latter test makes use of the fact that TLS and SESAME use the same key pair and X.509 certificate. Hence the unique identifier of the X.509 certificate in the TLS client identification data is compared with the XID value in the PAC. If the PAC is valid and belongs to the user, then the CGI decides to allow the requested page to be sent to the user. In a fifth step, the requested page to be sent to the user.

5. Disputed issues relating to the disclosure of D1

5.1 Would the skilled person reading D1 regard sections 4 and 5 as relating to the same embodiment?

5.1.1 This issue was raised before the first instance, the reasons for the appealed decision stating that the title of section 5, "Integration of SESAME and TLS", itself made it clear that combining sections 4 and 5 was foreseen. Also section 5 did not describe the details of the PAC because these had already been described in section 4. Furthermore section 5.1 stated that user authorization was provided by SESAME and TLS and that other services were provided by TLS in the traditional way. Section 4.1 pointed out the close resemblance between an attribute certificate (AC) and the PAC used in SESAME; see last paragraph on page 308.

5.1.2 The reasons for the appealed decision cite parts of section 4 of D1 (for instance, table 2 on page 308) as well as parts of section 5 (for instance, sections 5.2.2, 5.2.4 and 5.2.5) to argue that the subject-matter of claim 1 of the then main request was known from D1. The board considers however that the skilled person reading D1 would not have understood that sections 4 and 5 relate to the same embodiment and so can be combined. On the contrary, the skilled person would have regarded it as impractical to adopt the approach proposed in section 4 (TLS extensions for attribute certificates) because, for instance, there was a lack of available implementations of a correspondingly enhanced TLS and that this approach would have required changes to users' web browsers; see first two paragraphs in section 5. According to the second paragraph of section 5, section 5 sets out an alternative approach to that in section 4. In this context the expression "alternative" is understood to mean that the measures in section 5 replace those in section 4. The reasons for the appealed decision are based on the incorrect premise that a discussion of integrating TLS and SESAME in section 5 is synonymous with combining sections 4 and 5. In fact, section 4 deals with an extended form of TLS which could not be implemented, hence the need for an alternative approach in section 5. Moreover, although section 4 mentions the close resemblance between the AC and the PAC twice (see page 308, lines 3 to 6 and the last four lines), contrary to the argument in the reasons for the decision, section 5 explains many more details of PACs, in particular their structure, in sections 5.22, 5.23 and 5.24. The appellant has not disputed that, as stated twice on page 308 of D1, ACs and PACs are similar. However this does not mean that they are necessarily identical and the similarity cannot be equated with a suggestion that sections 4 and 5 are combinable.

5.1.3 Hence the board finds that the skilled person reading D1 would not have regarded sections 4 and 5 as relating to the same embodiment. An objection of lack of novelty based on D1 may only be based on what the skilled person would understand to be the same embodiment. It may well be that some features disclosed in section 4 are also present in the embodiment of section 5, but D1 does not identify which are such common features and which are not, and therefore, based on this document only, it cannot be said that the features mentioned in the decision as being disclosed in section 4 are clearly and unambiguously derivable as being also features of the embodiment of section 5.

5.2 Does the unique identifier of the requestor's X.509 certificate in the PAC and/or the user name in the AC known from D1 qualify as the "requestor certified reference" set out in the claims?

5.2.1 According to the reasons for the decision, both the unique identifier of the requestor's X.509 certificate in the PAC and/or the user name in the AC can be considered as the claimed "requestor certified reference", since the definition of "certified reference" given in paragraphs [0028], [0029] and [0065] of the description is general and can be interpreted broadly. The unique identifier (XID) of the requestor's X.509 certificate in the PAC is used to verify the identity of the client; see section 5.2.3, page 312, lines 6 to 5 from the bottom, and section 5.2.4, page 313, lines 11 to 16. Also the AC contains the user's name; see page 308, section 4.1, table 2, "Owner".

5.2.2 The appellant has disputed these arguments, stating that nothing in the PAC is certified by either the user/client or by the TLS server, so that the PAC does not contain a certified reference. The XID of the X.509 certificate is the identifier of the user given by the issuer of the certificate, and an XID and/or user name cannot be regarded as a certified reference in the absence of a mechanism for such certification. The CGI compares the XID value in the PAC sent by the user/client with the unique identifier of the X.509 certificate used by the client for authentification purposes, it being assumed that the client's X.509 certificate can be trusted by the application server.

5.2.3 To decide this point, it is first necessary to consider how the skilled person would understand the expression "requestor certified reference" in the context of the application. In doing this the effect of this feature and how it is to be achieved as described has to be taken into account, while recognising that the expression used in the claim may be intended to be interpreted more broadly. According to the application, the grantor (issuer) is able to delegate part of its rights to the requestor (beneficiary) so that it can act as a proxy on behalf of the grantor to access information about the grantor held by a service provider; see paragraph [0003], last three lines. To do this, the grantor issues an electronic document to the requestor to receive specified benefits through access controls at the service or information origin; see paragraph [0010]. The original independent claims all set out a requestor certified reference. According to paragraph [0023], the requestor certificate could, for instance, be derived from X.509 conformant signatures. The requestor certified reference is not meant to have global significance, as it is embedded in a structure that allows trust creation of the value. It is assumed that the requestor has created the reference and sent it to the grantor of the mandate prior to the creation of the mandate itself. A typical reference is a combination of URL and Public Key Certificate, but can include a customer account number; see paragraph [0029] and page 10, lines 7 to 13. According to the sentence bridges pages 16 and 17 and paragraph [0065], lines 8 to 9, the requestor certified reference may include a name combined with a password or a digital certificate. In the example shown in figure 4, in response to a request from the grantor, the requestor sends its public key certificate (406) which, together with the requestor's authorizations, is later digitally signed by the grantor to form the mandate, as shown in figure 6; see also paragraph [0045]. The board understands this example to mean that the requestor's public key certificate (406) is the claimed "requestor certified reference". Figure 7 and paragraph [0048] set out how the service provider checks the identity of the requestor before granting access to information about the grantor. This involves checking whether the requestor's public key certificate in the mandate corresponds to the public key of the person who signed the whole request, thereby preventing a valid mandate from being used by the wrong requestor.

5.2.4 This review of the use of the expression "requestor certified reference" in the application shows that the expression, when properly construed, must be understood more narrowly than stated in the reasons for the appealed decision. In the board's view the expression "requestor certified reference" must be understood as allowing the service provider to verify the identity of the requestor, thus preventing a valid mandate from being used by the wrong requestor. Consequently, as the appellant has argued, the present question seems to depend upon whether in D1 the CGI program of the application server can verify the identity of the requestor using the XID of the X.509 certificate, the appellant having argued that this is not the case.

5.2.5 The examining division has not introduced any evidence that the unique identifier in a X.509 certificate, as understood in D1, necessarily contains information, for instance a certificate, for verifying the identity of the user. (Nor, to the best of the board's knowledge of the standard, which must be considered to be part of the common general knowledge in the field, is that apparently the case.) Thus it is not directly and unambiguously derivable from D1 that the CGI program of the application server can verify the identity of the requestor using the XID of the X.509 certificate.

5.2.6 According to the reasons for the appealed decision, the user name in the AC in D1 can be seen as the claimed requestor certified reference; see "Owner" on page 308, section 4.1, table 2. According to page 308, lines 7 to 11, and figure 1 on page 309, the TLS protocol is modified so that the server can obtain an AC from an AC issuer detailing the client's privileges, the integrity of the AC being verifiable at the server. The AC structure is based on an X.509 certificate. As explained above in the context of the PAC, the unique identifier in the X.509 certificate in the AC would not qualify as the requestor certified reference either. Moreover the "Owner" field in table 2, which may contain the name of the entity to whom the attributes apply, does not directly and unambiguously disclose information with which the server can verify the identity of the requestor.

5.2.7 According to the reasons for the appealed decision, the combination of the AC and PAC, from sections 4 and 5 of D1, respectively, also discloses a "requestor certified reference". The board does not find this argument convincing, since, as set out above, D1 does not disclose combining the embodiments in sections 4 and 5.

5.2.8 Consequently the board accepts the appellant's argument that D1 does not disclose the "requestor certified reference" set out in the claims.

5.3 Does the issuer's signature of the AC in D1 qualify as the "grantor certified reference" set out in the claims?

5.3.1 According to the reasons for the appealed decision, this is the case, since the term "grantor certified reference" is to be understood broadly, paragraphs [0028] and [0065] in the description stating that the issuer certified reference 304 is typically a combination of a user name or customer account number and a Public Key Certificate and may, for example, include a name and password combination or a digital certificate. Thus the issuer's signature in the AC constitutes a "grantor certified reference"; see page 308, section 4.1, table 2. The AC is a digital certificate and thus a certified reference.

5.3.2 The appellant has disputed this finding, arguing that in D1 the issuer's signature is merely a hash of a document (the AC) and not a certified reference of the issuer. The appellant has also objected that the reasons for the appealed decision are inconsistent in that they assert that the AC is not only an electronic document, but also a certified reference.

5.3.3 To decide this point, it is again necessary to consider how the skilled person would have understood the expression "grantor certified reference" in the context of the application. In addition to the examples of grantor certified references given in the passages cited in the reasons for the appealed decision (see above), according to figure 6 and paragraph [0045], the only information stemming from the grantor in the request is due to the fact that the grantor digitally signs the requestor's public key certificate and authorizations before they are signed by the requestor.

This is understood to mean that the grantor computes a hash of the requestor's public key certificate and authorizations and encrypts the hash using its private key. Assuming that the private key has not been revealed to anyone else, the signature means that only the grantor can have given the signature. Paragraphs [0046] and [0047] explain how, in step 704 of figure 7, the service provider verifies the identity of the grantor to grant the requestor access to information about the grantor. Hence the skilled person would have understood that the "grantor certified reference" enables the identity of the grantor to be verified.

5.3.4 The "Issuer" in D1 who signs the AC cannot be equated with the Issuer/Grantor in the application; the former issues certificates concerning information on a user while the latter delegates rights to access information about him/herself. Hence the issuer's signature of the AC in D1 allows the identity of the AC issuer to be verified, which differs from the grantor's signature in the application, which allows the grantor's identity to be verified.

5.3.5 Hence the board accepts the appellant's argument that D1 does not disclose the "grantor certified reference" set out in the claims.

6. Novelty, Article 54(1,2) EPC 1973

It follows from the above analysis that the subject-matter of all independent claims of the main and auxiliary requests differs from the disclosure of D1 in at least a requestor certified reference and a grantor certified reference.

7. Inventive step, Article 56 EPC 1973

As pointed out by the appellant, although the appealed decision finds that claim 1 according to the main request lacks inventive step, it provides no reasons for this. The board accepts the appellant's argument that the first instance did not intend to raise an objection under Article 56 EPC 1973 against the main request. Whatever the intention of the first instance was, a full consideration of inventive step by the first instance has not yet taken place. Consequently the board refrains from going into inventive step for the purposes of this decision, beyond remarking that in the light of the analysis above a lack of inventive step would not follow from a combination of sections 4 and 5 of D1, both because the skilled person would not combine these alternative teachings and because such a combination would still not disclose the novel features.

8. Remittal, Article 111(1) EPC 1973

8.1 Since the application overcomes the grounds for refusal given in the appealed decision and inventive step has not yet been fully considered by the first instance, the board exercises its discretion to remit the case to the first instance for further prosecution. The appellant's conditional request for oral proceedings does not come into play, since the condition stipulated by the appellant, namely that the board be considering confirming the refusal of the application, is not fulfilled.

8.2 Remittal will also give the first instance the opportunity to consider the following issues:

8.2.1 In view of the analysis of D1 set out above, it seems that the reasons for the finding of lack of unity during search can no longer be maintained so that a further search for the unsearched claims will be required. According to the communication dated 3 December 2003 by the EPO as International Searching Authority, the application claimed two groups of inventions. These were those set out in claims 1 to 7, 31, 36 and 41 (first group) summarized as "Controlling access to information by means of a document digitally signed by the grantor and comprising grantor and requester references and access control rules" and those set out in the remaining claims, namely 8 to 30, 32 to 35, 37 to 40 and 42 (second group) summarized as "Controlling access to information by means of a document digitally signed by the grantor, comprising grantor and requester references, access control rules and an appended digitally signed request". Since, based on these summaries, the second group seems to set out subject-matter falling wholly within the first group, merely adding the feature that the document further contains an appended digitally signed request, it already seems doubtful whether the lack of unity objection can be maintained. Moreover, in view of the finding above that D1 does not disclose either a grantor certified reference or a requestor certified reference, it also seems that the finding in the communication that the common concept linking claim 1 with the claims of the second group, namely controlling access to information by means of a document digitally signed by said grantor and comprising a grantor certified reference, a requestor certified reference, and access control rules for said requestor wherein said grantor grants access to information stored in a computer system owned by another party to said requestor, was known from D1 is no longer tenable.

8.2.2 The limits of the expressions in all independent claims of both requests "grantor certified reference" and "requestor certified reference" seem to be indistinct. Firstly, it seems unclear whether the expression "grantor certified reference" covers self-certification by the grantor, particularly because paragraph [0028] states that "it is assumed" that certification is by the issuer’s company, telecommunication service provider or public authority. Similarly, in the case of the "requestor certified reference", paragraph [0029] seems to state that the reference is created by the requestor, implying that certification can also be by the requestor. Secondly, there is doubt as to what qualifies as a certified reference. Although paragraphs [0028] and [0029] give examples of a "grantor certified reference" in the form of a user name or a customer account number and a public key certificate and an example of a "requestor certified reference" in the form of a URL combined with a public key certificate, and the dependent claims set out in both cases a name and password combination optionally including a digital certificate, the technical features implied by a "certified reference" are uncertain.

8.2.3 It seems that, on a broad interpretation, the independent electronic document claim according to the main request could consequently be understood to cover a scanned version of a written document containing the two certified references, a rule and a grant of access by the grantor. On this interpretation, while the "electronic document" per se is a technical object, it might be considered that the other claimed features of this document, as presently specified, cover a presentation of information for business-related activities, namely producing credentials, laying down rules and delegating authority, aspects excluded from patentability under Article 52(2)(c) and (d) EPC, having an effect on the question of inventive step of the claim as a whole. Moreover the information about the grantor which is accessed by the requestor as proxy also seems to lack any technical aspects, indeed the description gives an example of access rights to financial data being granted to a proxy; see paragraph [0004].

8.2.4 In claim 33 of the main request and claim 21 of the auxiliary request the expression "method for access information" should presumably read "method for accessing information", thus leading to doubts as to the clarity of these claims, Article 84 EPC 1973.

8.2.5 The description seems to contain unnecessary statements, Rule 34(1)(c) EPC 1973, in paragraph [0001] (reference to another application), paragraph [0015] ("without departing from the scope and spirit of the inventive concepts disclosed herein") and paragraph [0070] ("the spirit of the appended claims").

Order

For these reasons it is decided that:

The decision under appeal is set aside.
The case is remitted to the first instance for further prosecution on the basis of the main request.

The Registrar: The Chairman:

Beschwerdekammern des Europäischen Patentamts
Boards of Appeal of the European Patent Office
Chambres de recours de l'Office européen des brevets

B. Atienza Vivancos D. Rees

Decision electronically authenticated