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

Datasheet for the decision of 26 June 2012

Case Number: T 0789/08 - 3.4.03

Application Number: 97951534.3

Publication Number: 965111

IPC: G07F 19/00

Language of the proceedings: EN

Title of invention:
Reliance server for electronic transaction system

Applicant:
CERTCO, LLC

Headword:
-

Relevant legal provisions (EPC 1973):
EPC Art. 56

Keyword:
-

Decisions cited:
T 0641/00

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

Case Number: T 0789/08 - 3.4.03

D E C I S I O N
of the Technical Board of Appeal 3.4.03
of 26 June 2012

Appellant: (Applicant)
CERTCO, LLC
280, Park Ave
New York, NY 10007 (US)

Representative:
Kenrick, Mark Lloyd
Marks & Clerk LLP
1 New York Street
Manchester, M1 4HD (GB)

Decision under appeal:
Decision of the Examining Division of the European Patent Office posted 26 October 2007 refusing European patent application No. 97951534.3 pursuant to Article 97(1) EPC 1973.

Composition of the Board:

Chairman: G. Eliasson
Members: V. L. P. Frank
T. Bokor

Summary of Facts and Submissions

I. This is an appeal from the refusal of application 97 951 534 for the reason that the subject-matter of the claims did not involve an inventive step (Article 56 EPC 1973).

II. At the oral proceedings before the board the appellant applicant requested that the decision under appeal be set aside and that a patent be granted on the basis of claims 1-48 of the main request, or claims 1-45 of the 1st auxiliary request, or claims 1-45 of the 2nd auxiliary request, all filed with the letter dated 23 May 2012, or on the basis of claims 1-45 of the 3rd auxiliary request, or claims 1-45 of the 4th auxiliary request, both filed during the oral proceedings before the board, or on the basis of claims 1-44 of the 5th auxiliary request, filed with letter dated 23 May 2012, or on the basis of claims 1-14 of the 6th auxiliary request, filed as 2nd auxiliary request with the grounds of appeal.

III. Claim 1 of the main request reads:

"1. An electronic transaction system wherein a certification authority (102) is arranged to generate electronic signals representing a digital certificate (110) associated with a subscriber (106) to the system, the digital certificate (110) representing assurance of an attribute of the subscriber (106), the system comprising:
a reliance server (104) arranged to receive electronic signals representing information regarding the digital certificate (110) issued by the certification authority

(102), the reliance server (104) arranged to issue electronic signals representing transactional assurance (118) to a relying party (108), the transactional assurance (118) being based at least on the digital certificate (110) and comprising a further digital certificate."

Claim 1 of the 1st auxiliary request reads:

"1. An electronic transaction system wherein a certification authority (102) is arranged to generate electronic signals representing a digital certificate (110) associated with a subscriber (106) to the system, the digital certificate (110) representing assurance of an attribute of the subscriber (106), the system comprising:
a reliance server (104) arranged to receive electronic signals representing information regarding the digital certificate (110) issued by the certification authority (102), the reliance server (104) arranged to issue electronic signals representing transactional assurance (118) to a relying party (108), the transactional assurance (118) being based at least on the digital certificate (110) and comprising a further digital certificate;
wherein the reliance server (104) is connectable to the certification authority (102), the reliance server (104) capable of receiving from the certification authority (102) electronic signals representing information regarding the digital certificate issued by the certification authority (102), and issuing electronic signals representing the further digital certificate (118) to the relying party (108), the issuing being based on the information received from the

certification authority (102) and on information provided by the relying party (108)."

Claim 1 of the 2nd auxiliary request reads:

"1. An electronic transaction system wherein a certification authority (102) is arranged to generate electronic signals representing a digital certificate (110) associated with a subscriber (106) to the system, the digital certificate (110) providing information identifying the subscriber (106) and representing assurance of an attribute of the subscriber (106), the system comprising:
a reliance server (104) arranged to receive electronic signals representing information regarding the digital certificate (110) issued by the certification authority (102), the reliance server (104) arranged to issue electronic signals representing transactional assurance (118) to a relying party (108), the transactional assurance (118) being based at least on the digital certificate (110) and comprising a further digital certificate;
wherein the reliance server (104) is connectable to the certification authority (102), the reliance server (104) capable of receiving from the certification authority (102) electronic signals representing information regarding the digital certificate issued by the certification authority (102), and issuing electronic signals representing the further digital certificate (118) to the relying party (108), the issuing being based on the information received from the certification authority (102) and on information provided by the relying party (108) and on further

information stored at or obtained by the reliance server (104)."

Claim 1 of the 3rd auxiliary request reads:

"1. An electronic transaction system wherein a certification authority (102) is arranged to generate electronic signals representing a digital certificate (110) associated with a subscriber (106) to the system, the digital certificate (110) providing information identifying the subscriber (106) and representing assurance of an attribute of the subscriber (106), the system comprising:
a reliance server (104) arranged to receive electronic signals representing information regarding the digital certificate (110) issued by the certification authority (102), the reliance server (104) arranged to issue electronic signals representing transactional assurance (118) to a relying party (108) in response to a request, the transactional assurance (118) being based at least on the digital certificate (110) and comprising a further digital certificate which provides the transactional assurance to the relying party;
wherein the reliance server (104) is connectable to the certification authority (102), the reliance server (104) capable of receiving from the certification authority (102) electronic signals representing information regarding the digital certificate issued by the certification authority (102), and issuing electronic signals representing the further digital certificate (118) to the relying party (108), the issuing being based on information in the request, on information with respect to a previous request based on the digital

certificate and on the information received from the certification authority (102)."

Claim 1 of the 4th auxiliary request reads:

"1. An electronic transaction system wherein a plurality of certification authorities (102) are arranged to generate electronic signals representing digital certificates (110) associated with subscribers (106) to the system, each digital certificate (110) providing information identifying the associated subscriber (106) and representing assurance of an attribute of the associated subscriber (106), the system comprising:
a reliance server (104) arranged to receive electronic signals representing information regarding digital certificates (110) issued by the certification authorities (102), the reliance server (104) arranged to issue electronic signals representing transactional assurance (118) to a relying party (108) in response to a request associated with one of said digital certificates, the transactional assurance (118) being based at least on the one of said digital certificates (110) and comprising a further digital certificate which provides the transactional assurance to the relying party;
wherein the reliance server (104) is connectable to the certification authorities (102), the reliance server (104) capable of receiving from the certification authorities (102) electronic signals representing information regarding the digital certificates issued by the certification authorities (102), and issuing electronic signals representing the further digital certificate (118) to the relying party (108), the

issuing being based on information in the request, on information with respect to a previous request based on the one of said digital certificates and on information received from the certification authorities (102)."

Claim 1 of the 5th auxiliary request reads:

"1. An electronic transaction system wherein a plurality of certification authorities (102) are arranged to generate electronic signals representing digital certificates (110) associated with subscribers (106) to the system, each digital certificate (110) providing information identifying the associated subscriber (106) and representing assurance of an attribute of the associated subscriber (106), the system comprising:
a reliance server (104) arranged to receive electronic signals representing information regarding one of said digital certificates (110) issued by the certification authorities (102), the reliance server (104) arranged to issue electronic signals representing transactional assurance (118) to a relying party (108) in response to a request associated with said one of said digital certificates for the assurance of the performance of an obligation, the transactional assurance (118) being based at least on the one of said digital certificates (110) and comprising a further digital certificate enclosing a statement of assurance of performance of the obligation, the further digital certificate attesting the authenticity of the statement;
wherein the reliance server (104) is connectable to the certification authorities (102), the reliance server (104) capable of receiving from the certification authorities (102) electronic signals representing

information regarding the digital certificates issued by the certification authorities (102), and issuing electronic signals representing the further digital certificate (118) to the relying party (108), the issuing being based on information in the request, on information with respect to a previous request based on the one of said digital certificates and on information received from at least one of the certification authorities (102)."

Claim 1 of the 6th auxiliary request reads:

"1. A computer-implemented method of managing reliance in an electronic transaction system in which a certification authority mechanism (102) issues a digital certificate (110) associated with a subscriber to the subscriber (106), the digital certificate (110) representing assurance of an attribute of the subscriber (106), the method comprising:
receiving electronic signals representing a transaction (112) associated with a subscriber (106), the transaction (112) comprising digitally signed information (114) and information regarding the digital certificate wherein the digitally signed information (114) is encrypted with a private key held by the subscriber (106) and the digital certificate comprises a corresponding public key;
creating a reliance request message (116) specifying at least one aspect of the transaction (112) upon which a relying party (108) intends to rely; and
causing electronic signals representing the reliance request message (116) to be sent to a reliance server (104) requesting a transactional assurance (118) for the aspect of the transaction upon which the relying

party (108) intends to rely, the reliance request message comprising information regarding the digital certificate (110) and the transactional assurance comprising a further digital certificate;
wherein the reliance server (104) is connectable to the certification authority mechanism (102), the reliance server capable of receiving from the certification authority (102) electronic signals representing information regarding the digital certificate issued by the certification authority mechanism (102), and issuing electronic signals representing the further digital certificate (118) to the relying party (108), the issuing being based on the information received from the certification authority mechanism (102) and on information provided by the relying party (108)."

IV. The following prior art documents are cited in this decision:

D1: "High-Tech Cure is at Hand for Internet Insecurities", Best's Review P/C, September 1996, pp. 98 and 100

D2: "Bricking up the 'Net to make it safe for business", CED: Communications Engineering & Design, August 1996, pp. 46, 48, and 49

D3: Utah Digital Signature Act, Utah Code Ann. title 46, chapter 3, 1996, §§ 46-3-101 to 46-3-104 (cited on page 1 of the application)

V. The examining division argued that:

– The subject-matter of the claims had technical character since it was directed to a computer implemented scheme. However, claim 1 was directed to an administrative scheme (subscriber assurance). Therefore, the claim was made up of technical and non-technical aspects. The non-technical aspects of claim 1 appeared to be:

> A transaction system comprising a certification authority generating data representing subscriber assurance of an attribute of a subscriber to the system, wherein a reliance entity received data representing information regarding the subscriber assurance issued by the certification authority, the reliance entity issuing data representing transactional assurance to a relying party, the transactional assurance being based at least on the subscriber assurance.

– The administrative system as described above considered on its own did not have technical character as it employed no technical means, caused no technical effect and solved no technical problem. Thus, when this scheme was considered independently from the technical aspects of the claim, it defined subject matter which was, under Article 52(2) and (3) EPC 1973, not regarded as patentable within the meaning of Article 52(1) EPC 1973.

– The technical character of the claim resided in that generic computing means were employed in place of the non-technical means for carrying out the non-

technical functions and thus provided an automation of the non-technical system. The technical aspects of the claim amounted to a conventional general purpose networked computer system. The application did not describe any technical interaction between the non-technical aspects and a conventional general purpose networked computer system. Nor could the examining division identify any technical inter-relationship from the application as filed. Therefore, the non-technical aspects were considered not to contribute to the technical character of the claimed subject matter.

– The closest prior art was considered to be a conventional general purpose networked computer system from which the subject matter of claim 1 differed merely through the use as a platform for the automation of the scheme described above. General purpose networked computer systems were so well known before the priority date of the present application not to require written evidence. The method described above was not relevant when assessing inventive step, as it did not contribute to the technical character of the invention. The person skilled in the art of data processing was used to the automation of non-technical schemes in a computer system. It was thus obvious to use a general purpose networked computer system to automate the administrative scheme, set out above. The subject-matter of claim 1 did not involve therefore an inventive step (Article 56 EPC 1973).

VI. The appellant applicant argued essentially as follows:

– The application was concerned with methods and systems for supporting reliance on digital certificates in computer networks. The application explained that an example of such a certificate was the International Telecommunication Union Standard X.509 certificate that certified the association of a public key used in public key encryption transactions with an individual with whom the public key was associated. The introductory part of the specification explained how digital certificates of the prior art were issued and used, and explained the inherent defects in the prior art approach. It was important to understand that the term "digital certificate" had a particular meaning in the field of computer networks, providing as it did a digitally signed record establishing a relationship between a particular identity and a representation regarding that identity. From the preceding discussion it followed that the invention had its basis in the technical field of assuring an attribute of a user in a computer network using digital certificates. This was the whole purpose of the invention as set out in the application.

– Documents D1 and D2 discussed the use of digital certificates in general terms. It was however not accepted that two journal articles, one published four months and the other published three months before the priority date of the application were sufficient to establish that the concepts described in the documents were part of the common general knowledge. It had to be borne in mind that the

application benefited from a priority date of December 1996. The state of network technologies at the priority date differed considerably from the present state of network technologies. As such, what seemed technically obvious with subconscious knowledge of the state of computer networking now would have been far from obvious in 1996.

– The technical problem solved by the invention was how to provide assurance of data associated with a subscriber in a computer network. It was common ground that at the date of priority electronic transaction systems based on digital certificates and systems using certification revocation lists (CRL) were known and such systems formed the closest prior art.

– In the case of the main request, the defined problem was solved by providing a reliance server that received information regarding a digital certificate associated with a subscriber in a computer network and generated by a certification authority, the reliance server providing transactional assurance, in the form of a further digital certificate, based on the digital certificate issued by the certification authority. In the prior art CRL based systems, there was no reliance server as the relying party contacted the certification authority directly. A shortcoming of a CRL system was that a party checking a digital certificate against a CRL typically did the checking with the certification authority that issued the fraudulent, invalid, inauthentic, etc. digital certificate. The claimed reliance server could help overcome that conflict of

interest by providing assurance to the relying party without reliance on a certification authority. The invention of claim 1 of the main request differed from the prior art not only in that a reliance server was provided but additionally in that the transactional assurance comprised a further digital certificate. Introducing a reliance server and consequent transactional assurance was counterintuitive and could not be said to be obvious.

– The independent claims of the 1st auxiliary request further specified that the reliance server was connectable to the certification authority and received information regarding the digital certificate from the certification authority. The claims further indicated that the reliance server issued the further digital certificate to the relying party based on the information received from the certification authority and on information provided by the relying party. It was disputed that the relying party had to tell the reliance server at least who the subscriber was, since the digital certificate associated with the subscriber already identified the subscriber. The reliance server might receive no information from a relying party if, for example, subscribers or certification authorities provided the information for issuance of the transactional assurance. As such, the information provided by the relying party was information additional to the information from the digital certificate associated with the subscriber identifying the subscriber.

– The claims of the 2nd auxiliary request further specified that the digital certificate provided information identifying the subscriber and that the issuing of the further digital certificate was based on further information stored at or obtained by the reliance server. The claims therefore clarified that the transactional assurance was based upon more information than the information already available from the digital certificate of who the subscriber was. There was nothing in any of the cited prior art to teach the use of further information to provide assurance of data and certainly nothing to teach or suggest use of further information stored at or obtained by a reliance server to provide the assurance of data.

– The claims of the 3rd auxiliary request further specified that the issuing was based on information in a request for transactional assurance, on information with respect to a previous request based on the digital certificate and on information from the certification authority. They therefore further specified the type of information on which the issuing was based. In particular, the claims made clear that information in the request for the transactional assurance and information from the certification authority were used, but additionally that information with respect to a previous request based on the digital certificate was used. The issuing of assurance was thus based upon collated information with respect to another request in combination with information in the request and information from the certification authority such that improved assurance of data was provided.

– The claims of the 4th auxiliary request further specified a plurality of certification authorities arranged to generate electronic signals representing digital certificates, that the reliance server was arranged to receive a request associated with one of the digital certificates and that the issuing of a further digital certificate was based on the one of the digital certificates. These claims therefore further clarified that the reliance server provided a mechanism through which data from a plurality of different certification authorities could be collated in order to provide improved reliance. In prior art CRL based systems the relying party contacted a single certification authority and there was nothing to suggest an intermediary connectable to a plurality of certification authorities so as to collate information from the certification authorities.

– The claims of the 5th auxiliary request further specified that the request was for assurance of the performance of an obligation and that the further digital certificate enclosed a statement of assurance of performance of the obligation, the further digital certificate attesting to the authenticity of the statement. They thus further clarified the function of the further digital certificate to provide assurance of an obligation for which the request requested assurance. It was therefore clear that the further digital certificate provided more than simply confirmation that the subscriber digital certificate was valid as in prior art CRL based systems. Claim 1 of this request

therefore further differed from the prior art in the nature of the information provided to the relying party.

– The claims of the 6th auxiliary request essentially further specified that the transaction comprised digitally signed information and information regarding the digital certificate wherein the digitally signed information was encrypted with a private key held by the subscriber and the digital certificate comprised a corresponding public key. Therefore the claim specified more than simply confirmation that the subscriber digital certificate was valid as in prior art CRL based systems.

Reasons for the Decision

1. The appeal is admissible.

2. *Background of the invention*

2.1 It is common ground that in conventional electronic transactions at least one of the parties to the transaction was in possession of a digital certificate issued by a certification authority. This party is named in the present application the subscriber to the system, while the other party to the transaction is the relying party. It is further common ground that digital certificates provided assurance of an attribute of the subscriber, eg his identity (see the present application's "Background of the Invention", Figure 3; D1, page 98, left hand column, 4th paragraph; D2, page 48. left hand column, 3rd paragraph).

2.2 The conventional electronic transaction system involved thus three actors: the certification authority and the two parties to the transaction, ie the subscriber to the system and the relying party.

3. *Main request*

3.1 Claim 1 of the main request specifies that the electronic transaction system mentioned above under point 2 further comprises a reliance server that receives information regarding the digital certificate (in the following the primary certificate) and issues transactional assurance to the relying party, the transactional assurance being based at least on the primary certificate and comprising a further certificate (in the following the secondary certificate).

The claimed electronic transaction system involves thus four actors: the certification authority 102, the subscriber 106, the relying party 108 and the reliance server 104; the electronic transaction 112 taking place between the subscriber 106 and the relying party 108 (Figure 3).

3.2 The board does not share the analysis of the features contributing to the technical character of the claim made by the examining division and agrees in this respect with the appellant applicant. In particular, the term *"transactional assurance"* appears to be particularly difficult in this context, as it covers embodiments having technical character (eg assuring the identity of the sender of a message using cryptography,

eg using public/private keys, or verifying the validity of a digital certificate) and embodiments that do not contribute to the technical character of the invention (eg assuring the credit limit of or the trust in a business partner).

The board will for the sake of the argument thus treat all the features of the claim as contributing to the technical character of the invention and interpret the term *"transactional assurance"* on hand of the embodiments making a technical contribution to the claim.

3.3 The application discloses in the section titled "Background of the Invention" that the certification authority (CA) issues and maintains a certification revocation list (CRL) containing revoked or temporarily suspended certificates (page 4). It is further disclosed that when a party to a transaction receives a digital signature (ie a digital certificate), it should check with the CA whether the corresponding certificate is still valid, ie that it is not listed on the CRL (page 5, lines 4 to 7).

The appellant applicant has not disputed that these features were part of the state of the art.

3.4 The system of claim 1 differs from the conventional method disclosed in the application, in which the relying party contacts the CA for verifying the validity of the certificate, essentially in that the relying party receives *"transactional assurance"* from a reliance server in the form of a secondary certificate.

3.5 The technical problem addressed by the method of claim 1 can thus be seen in how to improve the manner of obtaining transactional assurance.

3.6 As mentioned above, the term *"transactional assurance"* is interpreted by the board as comprising *inter alia* the verification in the CRL that the digital certificate is still valid and can be relied on. The reliance server thus takes over from the relying party the task of contacting the database of the CA and checking whether the primary certificate appears in the CRL. The transactional assurance delivered by the reliance server is based thus on the primary certificate as specified in the claim.

3.7 The reliance server issues the transactional assurance in the form of a secondary certificate to the relying party in order to assure who the sender of the information is. Digital certificates are encrypted with the reliance server's private key and can thus be decrypted with the reliance server's public key. In this manner the identity of the sender is established. This interpretation agrees with the definition of the secondary certificate given on page 36, lines 16 to 21 of the application, namely that *"A secondary certificate 118 is a message issued and digitally signed by a reliance server 104 or other certification authority mechanism 192"*.

3.8 The appellant applicant argued that documents D1 and D2 belonged to the infancy of digital certificates. They introduced digital certificates to electronic transactions, but did not suggest issuing further digital certificates as a vehicle for providing

transactional assurance (D1, page 98, leftmost and central column; D2, page 48, leftmost column).

The board is not convinced by this argument, since as stated in the cited passages of documents D1 and D2, the very purpose of digital certificates is to verify the identity of the sender. It is needless to say that a transactional assurance can only meet its purpose when the relying party is able to verify the identity of its issuer, ie that of the reliance server.

3.9 A skilled person would use a dedicated server specialized on handling the request of verifying with the CA the validity of the digital certificate for increasing the efficiency of this task, ie gaining transactional assurance, since a dedicated server is more efficient than a general one.

The board cannot recognize any inventiveness in transferring a task, ie checking the CRL, from one entity, ie the relying party, to another, ie the reliance server.

3.10 The board finds for the above reasons that the electronic transaction system of claim 1 of the main request does not involve an inventive step within the meaning of Article 56 EPC 1973.

4. *1st Auxiliary request*

4.1 Claim 1 of this request specifies further to the features of claim 1 of the main request that the reliance server is connectable to the CA, is capable of receiving information from the CA regarding the primary certificate and is capable of issuing the secondary certificate to the relying party, based on the information received from the CA and on information provided by the relying party.

4.2 However, the board's analysis of claim 1 of the main request already involved the features that the relying party forwarded the primary certificate to the reliance server, that the reliance server contacted the CA and checked whether the primary certificate was on the CRL, and that the reliance server issued the secondary certificate to the relying party on the basis of the answer received form the CA.

4.3 The appellant applicant contended that the information provided by the relying party was information additional to the information from the digital certificate associated with the subscriber identifying the subscriber. However, the board does not see a basis for this contention in claim 1, since the claim merely specifies that the issuing is based *inter alia* on information from the relying party. Forwarding the primary certificate to the reliance server is such information.

4.4 The appellant applicant further argued that the reliance server was a trusted broker and that it was counterintuitive to contact the CA for obtaining

transactional assurance, since it was the CA which had emitted the primary certificate to the subscriber.

However, as the board observed when discussing the main request, it was the recommended practice that the relying party contacts the CA for verifying that the primary certificate was still valid ("Background of the Invention", page 5, lines 4 to 7). Far from being counterintuitive, contacting the CA was the recommended course of action.

4.5 The board therefore finds that the electronic transaction system of claim 1 of the 1st auxiliary request does not involve an inventive step for the reasons presented with respect to claim 1 of the main request.

5. *2nd Auxiliary request*

5.1 Claim 1 of this request specifies further to the features of claim 1 of the 1st auxiliary request that *"the digital certificate providing information identifying the subscriber"* and that the issuing of the secondary certificate by the reliance server is based additionally *"on further information stored at or obtained by the reliance server"*.

5.2 The feature that the digital certificate provides information on the subscriber's identity is one of the reasons mentioned in documents D1 and D2 for using digital certificates. According to D2, *"In the electronic world, `digital certificates´ take the place of a physical piece of ID …"* (D1, page 98, left hand column, 4th paragraph; D2, page 48, left hand column, 2nd

and 3rd paragraphs). It is thus a standard feature of digital certificates.

5.3 The feature that the reliance server issues the secondary certificate on the basis of information stored at or obtained by the reliance server is very general, since the kind of information is neither specified nor qualified. The information stored at or obtained by the reliance server does not have to be information related to the subscriber, but may comprise eg the information that the relying party has a valid contract with the reliance server or that it is an authorized user of the system. Issuing the secondary certificate only if and when the relying party is up to date with its payments for the service is however a standard practice in the business world. The same is true for checking whether those requesting a service are authorized to do so.

5.4 The board therefore finds that the electronic transaction system of claim 1 of the 2nd auxiliary request does not involve an inventive step for these reasons and for the reasons advanced in relation to claim 1 of the main and 1st auxiliary requests.

6. *3rd Auxiliary request*

6.1 The electronic transaction system of claim 1 of this request differs from the conventional electronic transaction system acknowledged in the application and described above under points 2 and 3.3 essentially in that:

(a) a reliance server is used;
(b) the reliance server provides transactional assurance to the relying party by issuing a secondary certificate in response to a request;
(c) the issuing being based
  (i) on information in the request,
  (ii) on information with respect to a previous request based on the primary certificate, and
  (iii) on information received from the certification authority.

6.2 The main difference with respect to the electronic transaction systems of the main, 1st and 2nd auxiliary requests consists in that the secondary certificate is now issued based on additional information with respect to previous requests based on the primary certificate (ie feature (c)(ii)).

6.3 This feature corresponds, according to the appellant applicant, to the reliance server maintaining a record of the history of transactions (page 42, point 1.B.7). Consulting the transaction's history allows the assessment of the cumulative exposure to risk incurred by repeatedly relying on the primary certificate (page 14, lines 19 to 27). Such a transaction history is not required for a mere consultation of the CRL to confirm the validity of the primary certificate.

6.4 The board agrees with the appellant that the consultation of the CRL does not require keeping a database record of previous transactions. The presently claimed system goes therefore beyond such mere consultation.

However, the *"transactional assurance"* provided by the reliance server has now moved into the realm of business methods which do not contribute to the technical character of the invention. This was addressed under point 3.2 when discussing the interpretation of the term *"transactional assurance"*. Keeping records of the history of transactions with a specific party belongs to the realm of doing business. The concepts of trusted partners, cumulative risk or even commercial risk assessment underlying presently the *"transactional assurance"* provided by the reliance server are not features that contribute to the technical character of the invention, since they correspond to the tasks of a rating agency when assessing the reliability of commercial partners.

6.5 It was stated in decision T 641/00 (COMVIK, OJ EPO 2003, 352) that when a claim refers to an aim to be achieved in a non-technical field, this aim may legitimately appear in the formulation of the problem as part of the framework of the technical problem that is to be solved, in particular as a constraint that has to be met (Headnote, point 2).

6.6 The problem addressed by the electronic transaction system of claim 1 of the 3rd auxiliary requests can therefore be formulated as how to improve the task of providing transactional assurance to a relying party by evaluating the historical records of the subscriber.

6.7 The skilled person, ie an IT specialist, would incorporate into the reliance server a database that keeps records of the previous transactions for solving

the above posed problem. This is however a task that falls within the ambit of his normal activities. The board cannot recognize an inventive step in setting up and maintaining a database, since how to do this was known before the priority date of the application.

6.8 The appellant applicant further argued that it was unknown to provide the transactional assurance in the form of a digital certificate, in particular to provide an amount of money for which the risk was still acceptable. Conventional digital certificates only contained the identity of the subscriber and his public key.

6.9 The board is however not persuaded by this argument since document D3, the "Utah Digital Signature Act", defines under 46-3-103(26) a "Recommended reliance limit" as meaning the limit of an issuing certification authority's liability and financial responsibility specified in the certificate. It further specifies under 46-3-104(1) (j) that a certificate issued by a licensed certification authority shall contain the recommended reliance limit for transactions relying on the certificate. Thus including in a digital certificate an amount of money for which a risk was still acceptable was not only a theoretical possibility but indeed a legally regulated option under the Utah Act. This feature is thus part of the state of the art.

6.10 The board for these reasons cannot recognize the presence of an inventive step in the electronic transaction system of claim 1 of the 3rd auxiliary request.

7. *4th Auxiliary request*

7.1 The electronic transaction system of claim 1 of the 4th auxiliary request differs from the system of claim 1 of the 3rd auxiliary request essentially in that a plurality of certification authorities generate digital certificates associated with subscribers to the system and that the reliance server issues the secondary certificate also on the basis of information received from the certification authorities (CAs).

7.2 According to the appellant applicant issuing the secondary certificate on the basis of information provided by a plurality of CAs enhances the reliability of the transactional assurance, as it allows gathering as much information about the subscriber as possible. It encompasses moreover the checking of the reliability of the CAs themselves, since, as disclosed in the application, a CA is certified by a higher ranking CA, this going up until a root-CA (page 2, line 26 to page 3, line 14; Figure 2).

7.3 The board considers that in the system of claim 1 of this request the transactional assurance also comprises embodiments that contribute and that do not contribute to the technical character of the invention, as explained below.

The embodiment in which the information received from the plurality of CAs is used to verify the identity of the CA themselves, ie whether their identity has not been usurped, can be considered as having technical character, since it involves checking an identity on hand of cryptography.

On the other hand, the embodiment in which the information from the CAs is aimed at gathering information on the transactional performance and history of a subscriber is the activity of a rating agency, ie a business activity that does not contribute to the technical character of the invention.

7.4 However checking the identity of the CAs themselves in a hierarchical chain is a standard procedure of the state of the art as acknowledged in the application (pages 2-3, "Background of the invention"). On the other hand, the embodiments not contributing to the technical character of the invention have to be incorporated in the technical problem and therefore do not contribute to the inventiveness of the claimed system.

7.5 The board finds for these reasons that the electronic transaction system of claim 1 of the 4th auxiliary request does not involve an inventive step.

8. *5th Auxiliary request*

8.1 The electronic transaction system of claim 1 of the 5th auxiliary request differs from the system of claim 1 of the 4th auxiliary request essentially in that the secondary digital certificate issued by the reliance server encloses a statement of assurance of performance of an obligation and in that the secondary certificate attests the authenticity of the statement.

8.2 The board considers that providing assurance of the performance of an obligation is a feature that does not

contribute to the technical character of the invention, since it belongs to the field of performing business. This feature should appear, following decision T 641/00, in the formulation of the problem as part of the framework of the technical problem to be solved. The person skilled in the art, ie a programmer, would have no difficulty in implementing the statement using public/private key encryption so that the relying party may verify the validity of the statement. Furthermore, assuring financial liability is akin to the performance of an obligation, so that this feature is not inventive for the same reasons as in point 6.9.

8.3 The board finds for these reasons that the electronic transaction system of claim 1 of the 5th auxiliary request does not involve an inventive step.

9. *6th Auxiliary request*

9.1 Claim 1 of this request essentially casts the electronic transaction system of claim 1 of the 1st auxiliary request in the form of a computer-implemented method of managing reliance in an electronic transaction system. The differences with respect to claim 1 of the 1st auxiliary request reside, aside from the specification of method steps, in that:

(a) it is specified that a reliance request message is sent to the reliance server and in that

(b) the digitally signed information is encrypted with a private key held by the subscriber and the digital certificate comprises a corresponding public key.

9.2 The board, however, is of the view that the sending of a reliance request message to the reliance server is also implicit in all the electronic transaction systems of the previous requests. Furthermore, the asymmetric encryption method using public/private keys is known in the state of the art (D1, page 98, left hand column, 2nd paragraph; D2, page 46, right hand column, 8th paragraph).

9.3 The appellant applicant has not argued that the method of claim 1 of this request involved any substantive differences. The board's objections on the electronic transaction system of the previous requests are directed to the substance and not to the form of the claims. Casting the claim as a computer-implemented method does not address any of these objections.

9.4 The board finds for these reasons that the method of claim 1 of the 6th auxiliary request does not involve an inventive step.

Order

For these reasons it is decided that:

The appeal is dismissed.

Registrar | Chair

S. Sánchez Chiquero | G. Eliasson