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

Internal distribution code:

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

DECISION
of 20 January 2005

Case Number:	T 0052/02 - 3.5.3
Application Number:	89300117.2
Publication Number:	0328232
IPC:	H04L 9/00
Language of the proceedings:	EN

Title of invention:
Public key/signature cryptosystem with enhanced digital signature certification

Patentee:
Fischer, Addison M.

Opponents:
Alcatel SEL AG Zentralbereich Patente und Lizenzen
GIESECKE & DEVRIENT GmbH

Headword:
Enhanced digital signature/FISCHER

Relevant legal provisions:
EPC Art. 52, 56

Keyword:
"Inventive step - no"

Decisions cited:
-

Catchword:
-

Case Number: T 0052/02 - 3.5.3

DECISION
of the Technical Board of Appeal 3.5.3
of 20 January 2005

Appellant: (Opponent)	Alcatel SEL AG Zentralbereich Patente und Lizenzen Postfach 30 09 29 D-70449 Stuttgart (DE)
Representative:	Brose, Gerhard Zentralbereich Patente und Lizenzen Postfach 30 09 29 D-70449 Stuttgart (DE)
Appellant: (Opponent)	GIESECKE & DEVRIENT GmbH Prinzregentenstrasse 159 D-81677 München (DE)
Representative:	Dr. F. Klunker Klunker/Schmitt-Nilson/Hirsch Winzererstrasse 106 D-80797 München (DE)
Respondent: (Proprietor of the patent)	Fischer, Addison M. 60 14th Avenue South Naples, Florida 33940 (US)
Representative:	Dr. J. Dorner KUHNEN & WACKER Patent- und Rechtsanwaltsbüro Postfach 19 64 D-85319 Freising (DE)
Decision under appeal:	**Interlocutory decision of the Opposition Division of the European Patent Office posted 9 November 2001 concerning maintenance of European patent No. 0328232 in amended form.**

Composition of the Board:

Chairman:	A. S. Clelland
Members:	D. H. Rees R. Moufang

Summary of Facts and Submissions

I. Opponent 1 opposed European Patent No. 0 328 232 on the grounds that its subject-matter was not patentable within the terms of Articles 52(1), 52(2)(c) and 56 EPC (Article 100(a) EPC). Opponent 2 opposed it on the grounds that the subject-matter was not patentable within the terms of Articles 52(1) and 56 EPC (Article 100(a) EPC), and that its subject-matter extended beyond the content of the application as filed (Article 100(c) EPC). Among the documents cited by the opponents were

D1: G.J. Simmons, "An impersonation-proof identity verification scheme," "Advances in Cryptology - CRYPTO '87," ed. C. Pomerance, pages 211 to 215, Springer Verlag, Berlin, 1987.

D2: K. Rihaczek, "TeleTrusT-OSIS and communication security," "Computers and Security", vol. 6 no. 3, pages 206 to 218, Elsevier, Amsterdam, NL, June 1987.

II. Taking into account amendments made by the proprietor during the opposition proceedings, the opposition division found that the patent and the invention to which it related met the requirements of the EPC. The decision was given at oral proceedings held on 17 October 2001, with written reasons despatched on 9 November 2001.

III. The independent claim of the request on which the opposition division's decision was based reads as follows:

"1. In a communication system having a plurality of terminal devices (terminals A to N) coupled to a channel (12) over which users of said terminal devices may exchange messages, at least some of said users having a public key (30) and an associated private key (32), a method for managing authority by digitally signing and digital signature certifying a digital message to be transmitted to an independent recipient comprising the steps of:

generating at least a portion of said digital message (20);

digitally signing at least said portion of said message (40) with a user's private key;

associating with said message as part of the digitally signed portion thereof, an authorizing digital certificate for the associated public key (28, 116) of the respective user, said authorizing digital certificate having a plurality of digital fields created by a certifier, said authorizing certificate being created by the steps of:

specifying, in at least one of said digital fields, the public key of the certifier who digitally signs said authorizing digital certificate and

including in other of said digital fields an antecedent certificate of an antecedent certifier for said certifier, said antecedent certificate specifying the public key of said antecedent certifier who digitally signed his antecedent certificate, characterized in that

- in said at least one of said digital fields, there is included also a specification of the authority which is vested in the certifier and which has been delegated to the respective user;

- in said other of said digital fields there is included also a specification of the authority which has been granted to said certifier from said antecedent certifier; and

- on the side of an independent recipient of said message, an analysis of the information in said plurality of digital fields takes place for determining that the authority exercized [sic] by the respective user in signing the content of the message created by him was properly exercized by the user in accordance with the authority delegated by the certifier and that the certifier had been granted the authority to grant said delegated authority."

IV. Notice of appeal was filed, together with the appropriate fee, by Opponent 2 in a letter dated and received on 10 January 2002. A statement setting out the grounds of appeal, reiterating the objection that the claimed subject-matter did not involve an inventive step, and requesting therefore that the patent be revoked, was submitted on 11 March 2002. The respondent requested in return that the patent be maintained with the documents defined in the opposition division's decision, i.e. that the appeal be dismissed. Opponent 1 did not comment on the statement of grounds of the appeal.

V. The board issued an invitation to oral proceedings. A letter was received from Opponent 1 indicating that no-one would attend to represent it. At the oral proceedings the appellant requested that the decision of the opposition division be set aside and the patent revoked. The respondent requested that the appeal be dismissed. At the end of the oral proceedings the chairman closed the debate and announced the board's decision.

Reasons for the Decision

1. The only objection raised by the appellant to the patent in its amended form was that its claimed subject-matter did not involve an inventive step. In view of the outcome of the appeal the board sees no need to go into any other issues.

2. *The invention*

2.1 The patent is concerned with the field of cryptography, and in particular the use of public key cryptography to authenticate the source and integrity of a received message. Assuming a receiver is in possession of the public decryption key of a message sender, the process can be as follows. A "digital signature" is appended to the message prepared by the sender. This is created by first applying a known mathematical function (a "hash" function) to the contents of the message and then encrypting the resulting value using the sender's private key. The message is sent and the receiver calculates the same hash value of the message contents and applies the public decryption key of the alleged sender to the signature. If the hash value calculated by the receiver and the decrypted signature are equal, the receiver can be sure that the message does originate from the sender (or to be precise, someone in possession of the sender's private encryption key) and that the message has not been tampered with since it was signed.

2.2 The sender's public key may be conveyed to potential receivers by a variety of means external to the actual channel of communication. However, it is possible for the message itself to include the sender's public key, and for the receiver nonetheless to be sure that the message is authentic. This is done by including a "certificate" in the message. The certificate is in itself a message digitally signed by a "trusted authority" which specifies the sender's identity and public key. The receiver of a message extracts the certificate, checks the certificate's authenticity using the trusted authority's public key, and then uses the public key of the sender contained in said certificate to authenticate the message as a whole. In this way the receiver need only know the public key of a single central authority to authenticate a message coming from any (previously unknown) party.

2.3 It would be difficult for a single authority to deal with all requests for certification, especially as the process of certification can be expected to involve presentation of physical evidence of identity. This problem may be overcome by providing a hierarchy of certification. A single central trusted authority provides certificates to a number of local or specialised certification authorities, one of which provides a certificate to the final user, the sender discussed above. The sender includes not only the certificate obtained from the local authority, but also the certificate issued by the central authority to the local authority, which can be used to authenticate messages (certificates) prepared by the local authority. The receiver proceeds iteratively. The single public key which must be in the receiver's possession, that of the central authority, is used to authenticate the certificate issued to the local authority. The public key of the local authority contained in that certificate is then used to authenticate the certificate issued by the local authority to the sender, and the public key contained in this second certificate is used to authenticate the message itself. Clearly this hierarchical approach can be extended to more than two layers.

2.4 It was not disputed by the active parties that document D2 discloses such a system, and further discloses all features specified in the pre-characterising part of present claim 1. Based on this prior art, the parties also agreed that the problem solved by the patent is "to expand the capability of digital signature certification" (see the published patent at page 3, lines 55 and 56). This problem is solved by providing in certificates an indication of the authorisation which has been given to the receiver of the certificate by its issuer. For example, a certificate might specify that the holder of the certificate is authorised to make purchases up to some monetary limit (patent page 7, lines 52 and 53). Alternatively, it might specify that the holder of the certificate is authorised in turn to make certifications on behalf of the issuer of the certificate, i.e. holds the role of the "local authority" with respect to the "central authority" in the paragraph above (patent page 7, lines 33 to 51). The patent envisages a hierarchy of such authorisations being passed down through the hierarchy of identification certificates known from D2, and the claimed subject-matter specifies at least two such authorisations in respective certificates, one defining the authorisation of a certifier, which has been granted by an "antecedent certifier", and one defining the authorisation of the user, i.e. the message sender (the first two characterising features of claim 1). By checking iteratively that each level is not granted more authorisation than that which the previous level is empowered to grant, the message receiver may be confident not only that the message is authentic, but that the sender is empowered to carry out whatever transaction is requested (as in the example in the patent at page 6, lines 1 to 3, of buying a software package on behalf of a company).

3. *Inventive step*

3.1 Document D2 is the closest available prior art to the claimed invention. As stated above and agreed by the active parties, it discloses all the features in the pre-characterising part of the independent claim, including a hierarchical system of certificates included within a message to provide authentication of the message (source and integrity). It does not discuss providing authorisation for the sender of the message to carry out a requested transaction.

3.2 Document D1 also discusses a system using digital signatures and incorporating certificates to identify unknown senders with confidence (page 211, line 21, to page 213, line 5). It includes a suggestion that authorisations should be included within certificates (page 212, lines 10 to 16, "An identifier ... consisting of ..., as well as any limitations on the authorization conveyed in the signed identifier, such as credit limits, expiration date, levels of access, etc."). It goes on to use an example, withdrawal of cash from an ATM, where authorisation is clearly necessary (page 212, line 36, to page 213, line 5).

3.3 Thus D1 clearly indicates a way of expanding the capabilities of digital signature certification, i.e. a solution to the problem discussed at point 2.4 above.

3.4 The respondent pointed out that D1 does not show authorisations hierarchically arranged in certificates within a message, as specified in the claim. It was argued that there were other ways of specifying an authorisation, e.g. by reference to an external source, or by including the authorisation in a top-level certificate and not repeating it in the certificates associated with the lower layers.

3.5 The board agrees that there are methods of establishing authorisation which refer to external sources. Thus for example in the case of a notary authenticating a signature in business transactions (which was frequently discussed in the proceedings), the sent document may include an authentication by, say, a consul, that the authenticator is indeed a notary; the receiver of the document will still at least in theory need to consult outside sources, such as legal texts, in order to establish that a notary is indeed empowered to authenticate a signature. However, the whole point of providing multiple certificates in a hierarchical authentication system is to obviate the necessity for such external references in the process of authenticating the sender's signature, so that a received message is self-contained apart from the single public key of the central trusted authority that the receiver must hold. In the board's judgement the person skilled in the art would follow the same aim in extending the certificates with authorisation information. The obvious way to do that would be to include authorisation information in each certificate, and to check at each level that the authorisation contained within the certificate is within the limits which the next step up in the hierarchy is allowed to delegate.

3.6 The other suggestion of the respondent, that the sender's authorisation might be included in the top-level certificate and not repeated in the lower-level certificates, would mean that every possible authorisation at the bottom level of the hierarchy would have to be "signed-off" at the top level. This would negate completely the hierarchical process of delegation of authentication put in place in D2, and hence the skilled person would reject this option, even if it came to mind.

3.7 Thus, the skilled person, applying the teaching of D1 to the system of D2 and applying the hierarchical approach of D2 to the authorisation information would without the exercise of inventive skill arrive at the invention as specified in the present independent claim.

3.8 The board remarks that some of the considerations above may depend on aspects of the management model of an organisation, rather than on technical issues. According to the case law of the Boards of Appeal, such non-technical aspects cannot contribute to inventive step. However, since the board in this case has come to the conclusion that the claimed subject-matter is obvious in the light of the prior art, the question whether non-technical aspects are involved is moot.

4. Since the subject-matter of the independent claim does not involve an inventive step, the respondent's only request is not allowable. The appeal is therefore successful.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The patent is revoked.

The Registrar: The Chairman:

D. Magliano A. S. Clelland