Internal distribution code:

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

Datasheet for the decision of 25 September 2013

Case Number: T 1824/11 - 3.5.05

Application Number: 03104388.8

Publication Number: 1536601

IPC: H04L12/58, H04L29/06

Language of the proceedings: EN

Title of invention:
Encryption method and system for emails

Patent Proprietor:
Totemo AG

Opponent:
Zertificon Solutions GmbH

Headword:
E-mail encryption/TOTEMO

Relevant legal provisions:
EPC Art. 54, 56

Keyword:
Novelty - main request (yes)
Inventive step - main request (yes)

Decisions cited:

Catchword:

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 1824/11 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 25 September 2013

Appellant: (Opponent)	Zertificon Solutions GmbH Landsberger Allee 117 10407 Berlin (DE)
Representative:	Tönnies, Jan G. Boehmert & Boehmert Anwaltssozietät Niemannsweg 133 24105 Kiel (DE)
Respondent: (Patent Proprietor)	Totemo AG Seestrasse 134a 8700 Küsnacht (CH)
Representative:	P&TS SA (AG, Ltd.) Av. J.-J. Rousseau 4 P.O. Box 2848 2001 Neuchâtel (CH)

Decision under appeal: **Decision of the Opposition Division of the European Patent Office posted on 27 June 2011 rejecting the opposition filed against European patent No. 1536601 pursuant to Article 101(2) EPC.**

Composition of the Board:

Chair: A. Ritzka
Members: P. Cretaine
D. Prietzel-Funk

Summary of Facts and Submissions

I. The appeal of the opponent is against the decision of the opposition division, posted on 27 June 2011, to reject the opposition against European patent No. 1 536 601, which was based on the opposition grounds of lack of novelty and inventive step.

II. The documents cited in the opposition proceedings included the following:

D1: US 2002/0169954,

D2: T. DEAN, W. OTTAWAY: "Domain Security Services using S/MIME", RFC 3183, IETF Standard Engineering Task Force, CH, 1 October 2001,

D4: US 2003/0131259.

III. Notice of appeal was received on 19 August 2011. The appeal fee was paid on the same day. With the statement setting out the grounds of appeal, received on 26 October 2011, the appellant (opponent 1) requested that the decision under appeal be set aside and that the patent be revoked on the grounds of lack of novelty and inventive step (Articles 52(1), 54 and 56 EPC) in view of D4. In addition, oral proceedings were requested as an auxiliary measure.

IV. With a letter dated 9 March 2012, the respondent (patent proprietor) filed claims according to auxiliary requests 1 and 2 (corresponding to the claims of auxiliary requests 1 and 2 submitted on 22 February 2011 in opposition proceedings before the opposition division). It requested as a main request that the appeal be dismissed, or that the patent be

maintained on the basis of the claims of any the auxiliary requests. Furthermore it requested oral proceedings if the main request were not allowed.

V. A summons to oral proceedings scheduled for 25 September 2013 was issued on 31 May 2013. In an annex to this summons, the board listed the points which had to be discussed during the oral proceedings and expressed its preliminary opinion that the claims of the main request were new having regard to the disclosure of D4.

VI. The opponent in the first instance Privatsphere AG withdrew its opposition by the letter dated 22 July 2013.

VII. With a letter dated 23 August 2013, the respondent submitted further arguments and maintained its previous requests.

VIII. By letter dated 13 September 2013, the appellant announced that it would not be attending the oral proceedings and suggested that the appeal be decided in a written procedure.

IX. Oral proceedings were held on 25 September 2013 in the absence of the appellant.

At the end of the oral proceedings, the decision of the board was announced.

X. Claim 1 as granted reads as follows:

"1. Encryption method for emails sent from a sender (1) in his private network to a recipient (6), comprising the following steps:

the sender (1) requests from an encryption system (16) in said private network a certificate corresponding to said recipient (6),
the encryption system (16) returns to said sender (11) a first, proforma certificate corresponding to said recipient (6), wherein the proforma certificate is generated or retrieved by the encryption system (16) for the recipient (6) and only used between the sender (1) and the encryption system (16),
the sender (1) sends with his email client (11) an outgoing email to said recipient (6) encrypted with said proforma certificate,
said email is forwarded through said encryption system (16),
said encryption system (16) decrypts said email using a private key corresponding to said certificate,
said encryption system makes the content of said email available to said recipient (6)."

The set of claims as granted further contains an independent claim for a corresponding system (claim 30) and an independent claim for a corresponding computer program (claim 37).

Reasons for the Decision

1. Admissibility of the appeal

The appeal complies with the provisions of Articles 106 to 108 EPC (cf. point III above) and is therefore admissible.

2. Non-attendance of a party at the oral proceedings

The appellant decided not to attend the scheduled oral proceedings. Pursuant to Article 15(3) RPBA, the board is not obliged to delay any step in the appeal proceedings, including its decision, by reason only of the absence at the oral proceedings of any party duly summoned who may then be treated as relying only on its written case.

In the present case, the appellant did not submit any further arguments in response to the board's communication under Article 15(1) RPBA and to the letters of the respondent. The board was thus in a position to take a decision at the end of the oral proceedings in exercise of its discretion according to Article 15(3) RPBA, based on the submissions of the appellant in the statement setting out the grounds of appeal and on the written and oral submissions made by the respondent.

3. Main request

3.1 Prior art

Although the decision under appeal considered that document D1 was the closest prior art (see Reasons 10.3.1), the appellant said in the statement setting out the grounds of appeal that it did not share this view (see point 4.a), and did not use D1 or D2 in its argumentation. Instead the appellant based its argumentation solely on document D4. Thus the board indicated in the annex to the summons to oral proceedings that the issues of novelty and inventive step would be examined with respect to the disclosure of document D4 alone, notwithstanding that the opposition division had based its decision regarding novelty on either document D1 or D2 and regarding

inventive step on either document D4 or D1 alone or in combination.

D4 discloses an encryption method for establishing a secure link between a client and a secure website based on the HTTPS protocol (see Figure 1), e.g. for exchanging bank details with the website. D4 is concerned with the problem of making it possible, despite the encryption, to scan the exchanged data for illegal content, such as computer viruses or data banned as a matter of company policy. To this end, D4 teaches to redirect the client's request to a proxy computer which returns to the client a certificate issued by itself or by a certification authority. Upon acceptance of the certificate by the client, symmetric encryption is initiated between the client and the proxy, based on the certificate. The proxy is then able to decrypt the data sent by the client for scanning and to re-send these data on a secure HTTPS connection to the secure website. D4 mentions in a single passage (see paragraph [0016]) that the transferred data could be an encrypted e-mail.

3.2 Novelty - Article 54 EPC

3.2.1 D4 is focused on website access through an HTTPS connection, while the transfer of e-mails is mentioned solely in a single sentence of the summary of the invention (see paragraph [0016]).

The single preferred embodiment described in D4 relates to the transfer of data via a secure network connection established between a client and a website server. Such a connection establishes a secure end-to-end "tunnel" between the client and the server which is maintained for the duration of the session. By using an HTTPS

protocol for establishing the connections between the client and the proxy and between the proxy and the server, data is encrypted between the client and the proxy and between the proxy and the server, based on symmetric keys used for the duration of a whole client-website session. In contrast, the process of sending an encrypted e-mail using an e-mail client, as used in the encryption method of claim 1, and as generally known in the art (see e.g. the S/MIME protocol), is not based on the establishment of an end-to-end "tunnel" between sender and recipient but rather on an asynchronous process where an e-mail is encrypted by the sender using the recipient's certificate, and stored and forwarded over several mail servers.

Therefore the board judges, contrary to what the appellant argued in writing, that a skilled person, in the light of the whole disclosure of D4, will not interpret paragraph [0016] as meaning that an encrypted e-mail is transferred using a conventional e-mail client. The skilled person will rather consider that the secure website of D4 acts, if the sent data is an e-mail, as a webmail server, and that an e-mail is transferred as data in the HTTPS-based session between client and website. In this technology, well-known at the priority date of the patent as argued by the appellant, all the e-mails sent within a client-website session are encrypted based on the certificate of the website acting as webmail server and not based on the certificates of the particular e-mail recipients themselves.

Further, D4 discloses that the encryption of data between client and proxy is performed using a symmetric key, securely exchanged between client and proxy using

a proxy certificate (see paragraphs [0032], [0035] and Figure 3, boxes 10, 12 and 18).

Therefore the board judges that the differences between the subject-matter of claim 1 and the disclosure of D4 are that:

- the exchange of e-mails between the sender and the recipient is based on **conventional e-mail communication technology, using an e-mail client;**

- the certificate requested by the sender and returned by the encryption system in the private network is a **certificate corresponding to the recipient of the e-mail;**

- the above-mentioned certificate is **only used** between the sender and the encryption system (D4 is silent about a further use of the same proxy certificate for another sender);

- the **e-mail** sent by the sender is **encrypted with** the above-mentioned **certificate** (i.e. using the public key included in the certificate instead of using a symmetric key exchanged using the public key, as disclosed in D4).

Therefore the subject-matter of claim 1 is new having regard to the disclosure of D4 (Article 54 EPC).

3.2.2 The appellant argued in writing that the use of an e-mail client was implicitly disclosed in D4. As mentioned above, the board does not agree with this interpretation of D4 and considers that D4 discloses, at most, the use of a webmail. Furthermore, the

appellant argued that the certificate returned to the client in D4 corresponds to the recipient of the e-mail. The board is not convinced by this argument since D4 explicitly describes that the proxy returns a "proxy certificate" that the client may accept or not (see Figure 3, boxes 10 and 12). D4 does not provide any disclosure that the proxy certificate could correspond to the recipient, as required by claim 1.

3.3 Inventive step - Article 56 EPC

The technical effects of the distinguishing features listed in point 3.2.1 above are that an e-mail sent by a sender to a recipient may be encrypted based on the recipient's certificate and securely transferred to the recipient, while giving the private network of the sender the possibility of decrypting the e-mail without the sender being aware of it.

The objective technical problem can thus be defined as how to adapt the system of D4 to enable encryption of e-mails by a sender while allowing content-checking that is transparent to the sender.

As mentioned in point 3.2 above, D4 describes exclusively data transfer between a client and a website, using an HTTPS-secured connection. If the transferred data is an e-mail, as suggested by paragraph [0016], the e-mail service used could thus only be a webmail service. For this reason the skilled person would be encouraged to solve the above-mentioned technical problem within the technical framework of the communication system described in D4, i.e. using client-server HTTPS technology, rather than changing to completely different technology using a conventional

e-mail client at the sender as argued by the appellant. Moreover, even if the skilled person were to make that change, he would have to implement the further steps of designing the proxy certificate of D4 to correspond to the recipient and be unique to the sender. These further steps are also not suggested by D4, which describes the use of a proxy certificate not linked to the recipient and which may be re-used for other senders.

The appellant further argued in its statement setting out the grounds of appeal that a skilled person would have been aware that, according to ISO Standard X509, a certificate corresponding to the recipient is required by a conventional e-mail client. The respondent argued that this teaching could not be accepted as representing common general knowledge at the priority date of the patent, since no supporting document had been filed by the appellant. However, even if this were the case, the board concurs with the respondent that the X509 standard requires that the certificate be used for the end-to-end encryption from sender to recipient. Therefore, the skilled person would not be led by the standard to use an X509-compliant certificate only for encryption between the sender and an encryption system in the sender's private network.

For these reasons the board judges that the subject-matter of claim 1 involves an inventive step (Article 56 EPC) having regard to the disclosure of D4. Independent claims 30 and 37 contain the same features as claim 1, expressed in terms of, respectively, a system and a computer program, and, as such, also meet the requirements of Article 56 EPC. The several dependent claims comprise further limitations and

fulfil the requirements of Article 56 EPC at least for the same reasons as the independent claims.

4. Auxiliary requests

Since the claims as granted meet the requirements of Articles 54 and 56 EPC, there is no need to consider the respondent's first and second auxiliary requests.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chair:

K. Götz A. Ritzka

Decision electronically authenticated