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 6 December 2013

**Case Number:** T 0632/10 - 3.5.06

**Application Number:** 05018650.1

**Publication Number:** 1643402

**IPC:** G06F21/00

**Language of the proceedings:** EN

**Title of invention:**
Long-term authenticity proof of electronic documents

**Applicant:**
SAP AG

**Headword:**
Re-signing electronic documents/SAP

**Relevant legal provisions:**
EPC 1973 Art. 56

**Keyword:**
Inventive step - (no)

**Decisions cited:**
T 0426/88, T 1688/08

**Catchword:**

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

**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 0632/10 - 3.5.06**

# DECISION
# of Technical Board of Appeal 3.5.06
# of 6 December 2013

**Appellant:**
(Applicant)

SAP AG
Dietmar-Hopp-Allee 16
69190 Walldorf (DE)

**Representative:**

Müller-Boré & Partner Patentanwälte PartG mbB
Friedenheimer Brücke 21
80639 München (DE)

**Decision under appeal:**

**Decision of the Examining Division of the European Patent Office posted on 12 November 2009 refusing European patent application No. 05018650.1 pursuant to Article 97(2) EPC.**

**Composition of the Board:**

| | |
|---|---|
| **Chairman:** | D. Rees |
| **Members:** | M. Müller |
| | C. Heath |

## Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, with written reasons dispatched on 12 November 2009, to refuse the European patent application no. 05018650.1. The decision referred in particular to the document

D1: Schneier B., "Applied Cryptography", John Wiley & Sons, 1996, pp. 38-40,

and found a main and two auxiliary requests to lack an inventive step over D1 in view of a document labelled D4 and common knowledge, Article 56 EPC 1973.

II. Notice of appeal was received on 13 January 2010, the appeal fee being paid on the same day. A statement of grounds of appeal was filed on 17 March 2010. The appellant requested the decision to be set aside and a patent to be granted based on the main, first or second auxiliary request as subject to the decision or based on a set of claims according to a third, fourth or fifth auxiliary request as filed with the grounds of appeal, apparently in combination with the drawings and the description as originally filed.

III. With a summons to oral proceedings the board made reference to the German Signature Law (Signaturgesetz SigG) and the corresponding Ordinance on Electronic Signatures (Signaturverordnung SigV) as set out in the newly introduced documents

SigG: "Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)", entry into force 16 May 2001, Bundesgesetzblatt I 876, 21 May 2001, and

SigV: "Verordnung zur elektronischen Signature (Signaturverordnung - SigV)", entry into force 16 November 2001, Bundesgesetzblatt I 3074, 21 November 2001,

and gave its preliminary opinion that the claimed invention lacked an inventive step over D1 in view of especially § 17 SigV. A number of clarity objections were also raised.

IV. In response to the summons, the appellant replaced the previous requests by amended claims 1-31 according to a new main request, claims 1-30 according to new first and second auxiliary requests and claims 1-29 according to new third and fourth auxiliary requests.

V. Claim 1 according to the main request reads as follows:

"A computer-implemented method for providing long-term authenticity proof of an electronic document,

wherein said document is digitally signed with a digital signature and wherein said digital signature of the electronic document is constructed in a method which comprises calculating a hash value of the electronic document, and

wherein the method for providing long-term authenticity proof comprises archiving of the electronic document and its digital signature,

wherein the electronic document is stored in a first data archive, and

a hash information data comprising information about the hash value of the electronic document is stored in a second data archive which is different from the first data archive,

characterized in that

the first data archive is a standard archive for storing data and the second data archive is a re-sign archive different from the standard archive for a later re-signing of the hash information data stored in the second data archive,

said digitally signed electronic document is re-signed by providing a new digital signature to the hash information data stored in the second data archive and storing the re-signed hash information data in a data archive, and

wherein the hash information data comprises the hash value of the electronic document and the digital signature of the electronic document."

Claim 1 of the first auxiliary request coincides with claim 1 of the main request with the following text added to its end:

"... and wherein a hash information data stored in the second data archive comprises a reference to the corresponding electronic document for a later retrieval of the electronic document for proving the authenticity of the electronic document in a verification process."

Claim 1 of the second auxiliary request coincides with claim 1 of the first auxiliary request with the following further text added to its end:

"... and wherein the re-signed hash information data comprises a time stamp from a trusted third party."

Claim 1 of the third auxiliary request coincides with claim 1 of the second auxiliary request with the following further text added to its end:

"... and wherein the electronic document stored in the first data archive is a set of electronic documents which comprises a plurality of single electronic documents, particularly numerous single electronic documents."

Claim 1 of the fourth auxiliary request coincides with claim 1 of the third auxiliary request with the following further text added to its end:

"... wherein a hash value for each of the set of electronic documents, a reference to each of the set of electronic documents and a description of one or more algorithms used to calculate the hash values are stored in a document (B) and the document (B) is stored in the second data archive, and

wherein the re-signing of the digitally signed electronic document includes time stamping the document (B) stored in the second data archive by a trusted third party."

Each of the sets of claims also comprises two independent computer system claims and an independent use claim formulated by reference to *inter alia* respective claim 1.

VI. Oral proceedings were held on 6 December 2013. At their end, the chairman announced the decision of the board.

## Reasons for the Decision

*Admission of late-filed requests*

1. Compared with the previous version, the claims according to the present main and first to third

auxiliary requests were amended to overcome the clarity objections raised with the summons to oral proceedings, and the board accepts the claims according to the fourth auxiliary request as a genuine attempt to overcome the board's inventive step objection. The board therefore exercises its discretion under Rule 13 (1) RPBA to admit the new requests into the procedure.

*The invention*

2. The application relates to the question of how to provide long-term authenticity proof of electronic documents based on what is known as "electronic signatures" or, equivalently, "digital signatures" (see *e.g.* the original application, p. 4, 2nd par.).

2.1 An electronic signature is typically generated based on a hash value calculated from the electronic document and encrypted with a private key of the signing party. Users of the document can validate the signature by decrypting the signature with the public key of the signing party and comparing the value so-obtained with a hash value re-generated from the document. In case of a match the document is deemed to be authentic. Public keys and corresponding certificates may have a limited validity or may be revoked because the private key has become publicly known or safer encryption methods have become standard (see also p. 3, 2nd par.). Also the associated digital signatures may thus become invalid.

2.2 The application explains that in Germany electronic signatures may be acknowledged as documents in the legal sense if they comply with the German signature law (p. 2, 2nd par.). The relevant law is the above-mentioned German Digital Signature Law SigG and its Ordinance SigV, in view of the priority date of the present application both in their versions issued in 2001. The application further explains that for certain kinds of documents a proof of authenticity over many years is required, and that to this end it is prescribed to re-apply "secure methods and algorithms ... periodically by re-signing or time-stamping the electronic document and its digital signature" (see p. 5, last par. - p. 6, 2nd par.).

2.3 The application states that in state of the art time stamping processes the document itself must be available for the time stamping process (p. 6, lines 25-28). This is said to be inefficient, require expensive archiving technology, and be unsafe as it requires the handling of the electronic document (p. 6, lines 28-31). The invention sets out to address this problem.

2.4 The claimed invention (claim 1 of the *main request*) specifies that the electronic document is stored "in a first data archive" and "hash information data" is stored "in a second data archive ... different from the first" one. In the characterising portion, the first archive is referred to as "standard archive", the second one as a "re-sign archive". It is further claimed that "a new digital signature [is provided] to the hash information data" and stored in "a data archive", and it is specified that the "hash information data comprises the hash value ... and the digital signature of the electronic document".

2.5 In claim 1 of the *first auxiliary request* it is further specified that the "hash information data" comprises "a reference to the corresponding electronic document for a later retrieval of the electronic document".

In claim 1 of the *second auxiliary request* it is yet further specified that the "re-signed hash information data comprises a time stamp from a trusted third party".

Claim 1 of the *third auxiliary request* contains the additional requirement that the electronic document "is a set of electronic documents which comprises a plurality of single electronic documents".

Claim 1 of the fourth auxiliary request further defines a so-called "document (B)" which comprises for each of the set of documents a reference, the hash value and "a description of" the used hashing algorithms, and which is time-stamped as a whole.

*The prior art*

3. D1 is a short excerpt of a standard text book on cryptography.

3.1 It explains that signing long documents may be inefficient and that, therefore, hash functions are used to map documents to a short hash value which is signed instead of the document. For mathematical reasons, the signature of the hash can safely be "equated" with the signature of the document (see p. 38, lower half).

3.2 D1 further discloses that hashing in this context also increases privacy by making it possible that the signature is kept separate from the document. A central database could just store the hash values while the document could be kept secret elsewhere. The central database is disclosed to perform the time-stamping and the authentication (see p. 39, first full par.). It is further disclosed that a time-stamp is effectively a digital signature including date and time information (see p. 38, 5th par.).

4. The relevant regulations of the German Signature Act are *§§ 2 and 6 SigG as well as § 17 SigV* which, for ease of reading, are reproduced here:

*§ 2 SigG - Begriffsbestimmungen*

Im Sinne des Gesetztes sind

1. "elektronische Signaturen" Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen,

...

*§ 6 SigG - Unterrichtspflicht*

*(1) Der Zertifizierungsdiensteanbieter hat den Antragsteller nach § 5 Abs. 1 über die Maßnahmen zu unterrichten, die erforderlich sind, um zur Sicherheit von qualifizierten elektronischen Signaturen und zu deren zuverlässiger Prüfung beizutragen. Er hat den Antragsteller darauf hinzuweisen, dass Daten mit einer qualifizierten elektronischen Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.*

...

*§ 17 SigV - Zeitraum und Verfahren zur langfristigen Datensicherung*

*Daten mit einer qualifizierten elektronischen Signatur sind nach § 6 Abs. 1 Satz 2 des Signaturgesetzes neu zu signieren, wenn diese für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind. In diesem Falle sind die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen* *oder der zugehörigen Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen. Diese muss mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen.*

*Objective technical problem*

5. D1 discloses all features of the preamble of claim 1 (all requests) but is not concerned with providing long-term authenticity proofs (see grounds of appeal, p. 13, 1st par.). As a consequence, D1 also does not disclose that or how a document should be re-signed as specified in the characterizing portion of claim 1 (all requests).

5.1 Yet, the board disagrees with the appellant that D1 teaches away from considering long-term authenticity proofs because hash functions are disclosed to be very safe (see p. 38, last par.). Apart from the fact that hash functions have been cracked despite their high safety, a digital signature may also become useless for other reasons, *e.g.* because a private key has leaked.

5.2 Any developer of digital signature software for the German market at the relevant priority date had to comply with the German Signature Law, and developers interested in providing software supporting long-term digital signatures had to comply with the German Signature Law, especially with § 17 SigV, quite independent of any technical considerations they might also have had. The board notes that the law applies independently of technical considerations even though the law itself relates to a technical issue.

5.3 The board therefore considers that an objective technical problem solved by the invention is to implement a digital signature system according to D1 suitable for long-term authenticity proof compliant with the requirements of § 17 SigV. This also appears to conform with the background of the invention as presented in the application (*loc. cit.*).

*Relevance of a German law for the assessment of inventive step of a European patent*

6. During oral proceedings, the appellant argued that the German Signature Law might not be relevant for a European patent application such as the present one for which states other than Germany may be designated, because, as the board understands the argument, compliance with German law is of no concern outside Germany.

6.1 The board remains unconvinced by this argument for two reasons.

6.2 Primarily, an objective assessment of inventive step prohibits any differentiation between skilled persons according to their nationality, residence, location or language (see also T 426/88, OJ EPO 1992, 427, reasons 6.4.; T 1688/08, unpublished, reasons 4). Thus, even if an invention happened to be obvious only for skilled persons of German nationality or residence, it would still lack an inventive step in the sense of Article 56 EPC 1973.

6.3 Moreover, the German Signature Law is available and accessible beyond its region of validity. Digital signature software for the German market must comply with the German Signature Law. Compliance must be ensured by any developer of such software, independent of its own nationality or residence. The fact that the German Signature Law is valid only within Germany thus has no bearing on its status as prior art or its relevance for the assessment of inventive step outside Germany.

*Inventive Step*

*Main request*

7. D1 discloses an archival system which does not store the electronic document, but only its hash value in a central database (*loc. cit.*), *i.e.* in a "second data archive" as claimed. In this scenario, the hash value "represents" the document which the copyright owner prefers to keep secret in his or her own, separate local storage, *i.e.* in a "first data archive" as claimed.

7.1 § 17 SigV prescribes that a digital signature system suitable for long-term authenticity proof must be equipped to re-sign "the data" - *i.e.* the relevant electronic document - before the used algorithms or corresponding parameters become useless, based on "suitable new algorithms or corresponding parameters". § 17 SigV also prescribes that the new signature algorithm include earlier signatures and a qualified timestamp.

7.2 The skilled person modifying the system of D1 so as to comply with § 17 SigV would thus have to provide a way to renew digital signatures. Naturally, the skilled person would enhance the "second data archive", responsible already for the primary signature, so as to become a "re-sign archive".

7.3 The skilled person would understand from § 17 SigV that re-signing could use the old algorithms and parameters as long and to the extent to which they are still safe and permissible. As long as possible, the skilled person would obviously consider using the same algorithms for re-signing that were used to produce the original digital signature, in particular the same hashing algorithm.

7.4 The appellant argued that, according to D1, the two steps of generating a hash value and encrypting it were necessary parts of generating a digital signature (see nos. (1) and (2) on p. 38) and that D1 lacked any indication that either could be dispensed with. Also the requirement of § 17 SigV to re-sign "the data" had to be read as regenerating an electronic signature from the original document.

7.5 Therefore, so the argument, the available prior art taught the non-imaginative skilled person to refer to the original document whenever it had to be re-signed.

7.6 The board disagrees. As long as the same hashing algorithm is used, the skilled person would realize that it is not necessary to refer back to the original document because re-calculating the hash value would only produce the very same value which is already available. The skilled person would thus avoid this for obvious efficiency reasons and, in the system according to D1, for the additional reason that the original document is not or not easily accessible anyway. In the board's view this is also not in contradiction with § 17 SigV due to the fact that § 2(1) SigG provides a rather broad definition of the term "electronic signature".

7.7 The skilled person would find it obvious to produce a new digital signature based on the existing, old hash value and, because § 17 SigV so provides, would have to include the earlier digital signature.

7.8 The board concludes that claim 1 of the main request is an obvious implementation of the system of D1 compliant with § 17 SigV, and therefore does not involve an inventive step in the sense of Article 56 EPC 1973.

*First auxiliary request*

8. Even though according to D1 the electronic document is stored separately from the electronic signature it will, at some point, have to be retrieved. It is therefore obvious that some suitable "reference" be provided that enables such retrieval. This might be a contact address for the copyright owner just as well as an index into some storage location which might support automatic retrieval.

8.1 Neither D1 nor § 17 SigV discloses or prescribes that such reference be included in the new digital signature. The description is silent about the reason for doing this, but the board considers that the inclusion of any information in the digital signature protects that information against tampering.

8.2 In the board's judgement it would be evident for the skilled person that information relevant to retrieve a protected electronic document must also be protected against tampering: An archiving system such as that of D1 would not achieve its purpose if it were to authenticate a document via its hash value but then point an interested reader to the wrong document. The board therefore deems it obvious that all security-relevant information that happens to be stored in the "second data archive" be included in the digital signature, the reference included. Also § 17 SigV contains a pertinent hint in requiring that the new signature should "include" the old one.

8.3 The appellant submits that the "reference value does not only serve for retrieving the document [but also] for increasing security by enhancing the amount of structured data re-signed". The board first notes that if the provision of a feature is obvious as a means to achieve one effect, it does not become less obvious if it also has another effect. Beyond that, the board is not convinced that the inclusion of additional information into the data being signed can be said to increase security: The primary effect of signing additional information is that of providing authenticity proof for the additional information. Moreover it appears questionable whether a digital signature indeed becomes safer, or in what respect, when applied to additional information: By the same logic it would appear that a digital signature would be the safer the longer the signed electronic document. If a hashing algorithm were broken by, say, a collision attack, digital signatures relying on this hashing algorithm would be compromised independent of how much "additional information" the signed data contained.

8.4 Therefore, the board comes to the conclusion that also claim 1 of the first auxiliary request lacks an inventive step, Article 56 EPC 1973.

*Second auxiliary request*

9. During oral proceedings, the appellant confirmed that a time stamp according to the claim should be construed to subsume a normal electronic signature including suitable date and time information. This is, in fact, the

definition for time stamping given in D1 (*loc. cit.*). The board further considers that the central database according to D1 must be considered as a "trusted third party". Therefore, also claim 1 of the second auxiliary request lacks an inventive step, Article 56 EPC 1973.

Third auxiliary request

10. The appellant points out that D1 illustrates electronic signatures only by reference to small "documents", namely contracts or checks and thus neither discloses nor suggests that a signed document could "comprise a plurality of single electronic documents".

10.1 The board, however, considers it obvious for the skilled person that the principles of electronic signatures apply independent of the size and form of the document, and well-known that digital signatures have been applied to all sorts of documents (email, books, music, video, etc.).

10.2 In the board's judgment it is also obvious that "documents" to be protected as a whole may consist of several individual files, *i.e.* documents in the "technical sense": For instance, the individual chapters of an electronic book may be stored in separate files, as may be a contract and its potential annexes.

10.3 The board considers it obvious to apply a common electronic signature to all components of a document to be protected. Claim 1 of the third auxiliary request thus also lacks an inventive step, Article 56 EPC 1973.

Fourth auxiliary request

11. The claim makes reference to "a description of one or more algorithms used to calculate the hash values" but neither the claim nor the application as a whole define what kind of "description" is meant. The board construes this term broadly as any information relevant to identify the pertinent algorithms.

11.1 In order to validate the hash value encrypted in an electronic signature, it must be re-generated from the signed document. Therefore, a digital signature must identify, one way or another, the hashing algorithm relied on. Moreover, this information, too, must not be tampered with.

11.2 The board therefore considers for the above reasons (point 8.2) that it is obvious to include "a description of" the relevant algorithms in the hash information being signed.

11.3 The use of time-stamping and the joint signing of several documents was separately found obvious above. The board considers that this also applies to their combination.

12. Thus, also claim 1 of the fourth auxiliary request lacks an inventive step, Article 56 EPC 1973.

*Summary*

13. There being no allowable request, the appeal must be dismissed.

## Order

**For these reasons it is decided that:**

1. The appeal is dismissed.

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