Internal distribution code:

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

Datasheet for the decision of 14 March 2017

Case Number: T 1307/11 - 3.5.06

Application Number: 03293181.8

Publication Number: 1431861

IPC: G06F1/00

Language of the proceedings: EN

Title of invention:
Security token sharable data and synchronization cache

Applicant:
Assa Abloy AB

Headword:
Security token cache/ASSA ABLOY

Relevant legal provisions:
EPC 1973 Art. 56

Keyword:
Inventive step - (no)

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 1307/11 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 14 March 2017

Appellant: (Applicant)	Assa Abloy AB Klarabergviadukten 90 111 64 Stockholm (SE)
Representative:	Freischem & Partner Patentanwälte mbB Salierring 47-53 50677 Köln (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 24 January 2011 refusing European patent application No. 03293181.8 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	M. Müller
	G. Zucka

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, with reasons dispatched on 24 January 2011, to refuse European patent application No. 03 293 181.8 because claim 1 of both pending requests did not comply with Article 123(2) EPC. Moreover, in a section entitled "Obiter Dicta" it was explained why the independent claims of both requests lacked inventive step, Article 56 EPC 1973. Several documents were referred to in the decision, of which only one will be cited below, namely

D2: WO 02/48889 A1.

II. Notice of appeal was filed on 31 March 2011, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 31 May 2011. The appellant requested that the decision be set aside and that a patent be granted on the basis of claims 1-22 according to a main request or auxiliary request 1, or claims 1-21 according to auxiliary request 2, all as filed with the grounds of appeal, the other application documents on file being the description pages 2 and 2a as received on 24 January 2008 and the description pages 1 and 3-10 and the drawing sheets 1/10-10/10 as originally filed.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that the claimed invention according to all three requests lacked inventive step, Article 56 EPC 1973, over common knowledge in the art. Objections under Article 84 EPC 1973 were also raised.

IV. In response to the summons, with letter of 14 February 2017, the appellant filed an amended claim 1 of its main request.

V. Claim 1 of the main request reads as follows:

"A system for caching information retrieved from at least one hardware security token (5) wherein:

said at least one hardware security token (5) is in processing communications with a security token interface API (35), said at least one hardware security token (5) including information retrievable by said security token interface API (35),

said security token interface API (35) is functionally associated with a cache API (40), said security token interface API (35) including means for retrieving said information from said at least one hardware security token (5), means for sending said information to said cache API (40) and means for requesting said information from said cache API (40), and

said cache API (40) is functionally associated with at least one memory cache (45), said cache API (40) including means for storing said retrieved information in said at least one memory cache (45), means responsive to said request from said security token interface API (35) for locating and returning said information from said at least one memory cache (45) to said security token interface API (35) if the requested information is available from the at least one memory cache (45),

wherein said information in said at least one memory cache (45) is refreshed if it is not current, and

wherein said security token interface API (35) is notified to retrieve said information from the hardware security token (5) if said information is not available from the at least one memory cache (45)."

Claim 1 of auxiliary request 1 is identical to claim 1 of the main request, except for amendments to the preamble and the last paragraph which now read as follows:

"A system for caching information retrieved from at least one hardware security token (5) and for responding to requests for information received from at least one application (30), said system including said at least one hardware security token (5), a security token interface API (35), at least one memory cache (45) and a cache API (40), wherein:

...

it is determined if the requested information contained in said memory cache (45) is current and said information in said at least one memory cache (45) is refreshed if it is not current, and said security token interface API (35) is notified to retrieve said information from the hardware security token (5) if said information is not available from the at least one memory cache (45) in order to ensure that the requesting application (30) receives the latest version of information contained in said at least one hardware security token (5)."

Claim 1 of auxiliary request 2 is identical to claim 1 of auxiliary request 1, except for amendments to the last paragraph which now reads as follows:

"...

it is determined if the requested information contained in said memory cache (45) is current and said information in said at least one memory cache (45) is refreshed if it is not current, and said security token interface API (35) is notified to retrieve said information from the hardware security token (5) if said information is not available from the at least one memory cache (45) said cache API (40) further includes means for generating and storing a pseudo-entry if said requested information is not present in said at least one hardware security token (5)."

All three requests also contain an independent method claim 19 (or 18 in the case of auxiliary request 2) corresponding to system claim 1.

VI. Oral proceedings were held on 14 March 2017 as scheduled. At their end, the chairman announced the decision of the board.

Reasons for the Decision

The invention

1. The application is concerned with efficient access to memory on hardware security tokens.

1.1 Security tokens are explained to be "tamper-resistant hardware devices used to securely store digital credentials, cryptographic keys and other proprietary information". Otherwise they are only illustrated by

examples (see page 1, paragraph 3). A typical security token is a smart card.

1.2 When a token receives many requests in a short period of time, some requests may have to wait (page 1, lines 20-24). This may be aggravated by a slow serial data connection, but also by the need for exclusive access to the smart card to protect data integrity (see page 2, paragraph 1).

1.3 As a solution to this problem, the application proposes the provision of a "memory cache" for the token (see figure 1).

1.4 Applications (30) interact with the token via a suitable "token API" (35), also referred to and claimed as a "security token interface API". When an application requests information from the token, it will first be referred to the memory cache (45), via a corresponding "cache API" (40), to see whether the information is available in the cache and "current" (see page 8, paragraph 3). If it is, the information is retrieved and returned from the cache; otherwise the request is forwarded to the token.

1.5 The cache may also record token accesses which fail because the requested information is "not present" (or non-existent) in the token. In this situation, a "pseudo-entry" ("NA" for "not available") is generated and stored in the cache so that another request for the same information can be answered from the cache and the token need not be accessed again (see page 4, paragraph 3, page 9, paragraph 2, and page 10, paragraph 2). The description discloses that the pseudo-entry may be generated by the cache API (page 9,

line 9) or the security token API (page 4, lines 10-11, and page 10, lines 7-8).

The prior art

2. D2 relates to a cache for a web server. In its background section, it discloses caching to be a known technology to speed up frequent accesses to slow storage devices (page 1, line 9, to page 2, line 2). D2 also discloses that cached data may become "invalid" when the original data in the storage device has been changed, and that the data in the cache may then have to be refreshed (see paragraph bridging pages 1 and 2). The board considers these features of caching to belong to the common general knowledge in the art, and the appellant did not challenge that view.

Added subject-matter, Article 123(2) EPC

3. In its preliminary opinion, the board tended to disagree with the finding in the decision under appeal that the claims went beyond the content of the application as originally filed. In view of its conclusion on inventive step, however, this question can be left open.

Claim construction

4. Some of the central terminology in the claims is rather broad.

4.1 To begin with, the term "hardware security token" is not defined in the claims. According to the description, a broad range of hardware devices with some security functionality qualifies as a security token (see page 1 of the description). Additionally,

the claimed security token must contain "memory", but the type and size of this memory and how it arranges its contents remain undefined. In other words, the claimed security token must be construed as a memory device with some unspecified security functionality.

4.2 The independent claims of auxiliary request 2 refer to the situation in which "requested information" may not be "present" in the security token. It is not defined what type of information may be requested, what it means if the information is not present, and how the security token reacts to an attempt (via the token API) to retrieve information which is "not present" in the token.

4.2.1 The appellant stated that an application might try to access a memory location on the security token which does not exist because, say, the token is an old version with little memory. The board considers that, alternatively, the memory could store information associated with symbolic keys (such as name, address, password) and it may happen that for some such key ("address", say) no entry exists, or that a placeholder value is stored (e.g. "NIL"). The board takes the view that none of these interpretations is excluded by the claim language.

4.2.2 The appellant further suggested that the security token might not respond at all to an attempt to retrieve information which is "not present" and that, in this case, the security token interface API might have to detect the absence of the requested information by a time-out mechanism. The board however considers that alternatives are equally possible. For instance, the security token might return an error message or set an error flag, or it might generate and return a

placeholder value. A further alternative is that the security token might return the placeholder value stored in memory; in the latter case, one might say that the information was "present" from the perspective of the security token ("NIL" being a special value but a value nonetheless) but "not present" from the perspective of the requesting application ("NIL" meaning the absence of useful information).

4.2.3 In the board's view, the claims and the application as a whole contain no information which could exclude any of the above interpretations. The appellant did not challenge the board on this point.

4.3 The "pseudo-entry" referred to in claim 1 of auxiliary request 2 is, its name notwithstanding, an "entry" in the cache, just like any other. This is confirmed by the application itself (see page 4, lines 12-13). The board therefore takes the view that the cache itself need not be modified to accommodate a "pseudo-entry". The appellant argued during oral proceedings that the claimed cache was somehow "extended" over the memory in the security token. The board disagrees. Caches are not meant to hold a copy of the entire memory. Rather, only a small part of the memory is actually held in the cache. This means in particular that a cache need not be "extended" in any particular way to enable it to hold a "pseudo-entry" associated with the reference (address or key) to some "non-existent" information.

Inventive step

Main request

5. From common general knowledge on caching, the subject-matter of claim 1 differs in that

(a) the data being cached is stored in the memory of a "hardware security token",
(b) the security token is accessed via a "security token API" and
(c) the cache is accessed via a "cache API".

5.1 As regards feature (a), the board takes the view that the idea of providing a cache for memory on a security token is, in itself, obvious. As explained above, the claimed "hardware security token" is in particular a slow memory device. Caching was an established technology for speeding up access to slow memory devices. Therefore, in the board's judgement, the skilled person would not hesitate to use a cache for a "hardware security token" if the cost of the cache was justified by the gained speed.

5.2 As regards features (b) and (c), the board considers that the provision of APIs is a matter of workshop practice for a person with the appropriate programming skill.

5.3 Thus the board concludes that claim 1 of the main request lacks inventive step over common knowledge in the art, Article 56 EPC 1973, and so does claim 19.

Auxiliary request 1

6. Claims 1 and 19 of auxiliary request 1 include clarifications that the appellant considers "unnecessary", except that they address some of the examining division's concerns with respect to clarity (see grounds of appeal, page 8, paragraph 5). The amendments did not give rise to additional arguments by the appellant in favour of inventive step. Therefore, the above inven-

tive-step assessment also applies to the independent claims of the auxiliary request, which, hence, are also found to lack inventive step, Article 56 EPC 1973.

Auxiliary request 2

7. The additional features in claims 1 and 19 imply that applications may request information which is "not present" in the token. The board considers this to be a given, i.e. to be part of the problem the invention is meant to address rather than in itself a part of the solution. The claims leave open how the token reacts to such a request.

7.1 The appellant suggested during oral proceedings that the token might not respond to such a request at all. In this situation, the claimed pseudo-entry would be generated in place of the response of the token, typically after a time-out has been detected. According to the appellant, the claimed pseudo-entry made the token interface more robust with regard to the behaviour of the token when requested to provide absent information.

7.2 The board accepts the possibility of the above scenario but notes that the claimed "robustness" is achieved by the generation of a response (e.g. "NA") after a time-out and not by the fact that this response is cached. The board also considers that time-out mechanisms of the described type were well-known in the art, too.

7.3 More importantly, however, the board notes that an inventive step cannot be acknowledged on the basis of a merely potential advantage for a security token with

properties which are neither claimed nor disclosed in the application.

7.4 The board considers it obvious that a token requested to provide absent information will respond in some way, either with an error message or with a special value (e.g. "NIL", ".", "NA" or "NaV").

7.5 The claims can be interpreted as specifying essentially that this response is cached just like any "present" information.

7.6 That the pseudo-entry is generated after the token has been accessed means in particular that the token response is not cached directly but replaced with an "entry" value. The appellant did not explain what technical problem that might solve; nor does the application give any hint in this regard. The appellant also did not argue that it was crucial in this regard whether the cache API or the security token interface API generated the pseudo-entry.

7.7 The board takes the view that the caching of the token response to "absent" information achieves the effect of speeding up requests for absent information in precisely the same way as a "standard" cache speeds up access to "present" memory content. In effect, the token response is cached in both cases, whatever it may be.

7.8 The board considers this to be an obvious use of the well-known technique of caching.

7.9 In summary, claims 1 and 19 of auxiliary request 2 are also found to lack inventive step over common general knowledge in the art, Article 56 EPC 1973.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated