Internal distribution code:

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

Datasheet for the decision of 1 August 2017

Case Number: T 1758/14 - 3.5.06

Application Number: 09156290.0

Publication Number: 2112613

IPC: G06F21/20

Language of the proceedings: EN

Title of invention:
Restricted use information cards

Applicant:
EMC Corporation

Headword:
Information cards/EMC

Relevant legal provisions:
EPC Art. 84

Keyword:
Claims - clarity (all requests, 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 1758/14 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 1 August 2017

Appellant: (Applicant)	EMC Corporation 176 South Street Hopkinton, MA 01748 (US)
Representative:	Hanna Moore + Curley Garryard House 25/26 Earlsfort Terrace Dublin 2, D02 PX51 (IE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 10 April 2014 refusing European patent application No. 09156290.0 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	M. Müller
	S. Krischer

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, with reasons dispatched on 10 April 2014, to refuse European patent application No. 09 156 290.0 for lack of inventive step over document

D1: US 2007/204168 A1.

II. Notice of appeal was filed on 10 June 2014, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 29 July 2014. The appellant requested that the decision under appeal be set aside, and that a patent be granted on the basis of claims according to a main or an auxiliary request as filed with the grounds of appeal, the other application documents being description pages 1 and 2 as filed on 25 January 2011, and description pages 3-25 and drawing pages 1-11 as originally filed.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that the claims lacked clarity (Article 84 EPC). It also questioned whether the subject-matter of a claim that had been suitably clarified had a technical effect and was non-obvious over D1 (Article 56 EPC).

IV. In response to the summons, with letter dated 29 June 2017, the appellant filed amended claims 1-9 and 1-13 as new main and auxiliary requests respectively.

V. During the oral proceedings, which took place on 1 August 2017, the appellant filed further amended claims 1-9 and 1-13 as new second and third auxiliary requests respectively. The appellant also submitted two

new documents, which the board will refer to as follows:

D5: Cameron K, "The Laws of Identity", Microsoft, May 2005
D6: vibro, "UniqueID and PPID", blog entry dated 15 January 2017

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

"An information card system, comprising:
a client machine (200);
a relying party machine (130;
an identity provider machine (135);
the relying party machine being adapted to send (645) a security policy (650) including metadata specifying restricted use policies that are supported by the relying party to the client machine;
a card selector (205) on the client machine configured to receive a selection of a restricted use information card (220, 460) satisfying the security policy wherein the restricted use information card identifies a user of the client machine and includes an identifier (315) for the relying party (130), and wherein the restricted use information cared includes restricted use metadata describing a use restriction (310) applicable to the identified user at the relying party;
a transmitter (215) on the client machine configured to send a request for a security token (660) associated with the restricted use information card to at least one identity provider (135) machine, the security token uniquely identifying the user with a unidirectional identifier being a unique-id claim (670), which is relying party specific and provides assurances to the

relying party that the user is not using multiple personae from that identity provider,

the identity provider machine being adapted to generate the unique-id claim;

a received (210) on the client machine configured to receive the security token from the at least one identity provider (135); and

the transmitter being further configured to send the security token to a relying party machine."

In claim 1 of the (first) auxiliary request "a broker machine (135)" has been introduced as an additional component of the claimed information card system, reference numbers 645, 650 and 660 have been replaced by 545, 550 and 560 respectively; new reference numbers 555 and 565 have been introduced; and the last two lines ("the transmitter ...") have been replaced by the following text:

"... the transmitter on the client machine configured to send (570) the security token to a broker machine

wherein a restriction-id claim is generated by the broker machine (510), identifying or describing a restricted use policy (450) that was used by the broker to decide whether or not to issue a brokered security token (580);

the broker machine being adapted to send (575) the brokered security token (580) to a relying party machine (130)."

Claim 1 of the second auxiliary request differs from claim 1 of the main request in that at the end of the passage introducing the "unique-id claim" the following phrase has been added:

"... by generating the unique-id claim once, storing the unique-id claim, and using the stored claim for all subsequent requests for security tokens to the said relying party; ..."

Claim 1 of the third auxiliary request differs from claim 1 of the (first) auxiliary request in that the same addition has been made with regard to the unique-id claim and that, at the end of the claim, the following phrase has also been added:

"... such that for each security token the broker receives from a particular user of a client machine, the broker supplies the same unique identifier to the relying party in the brokered security token (580)."

All requests also contain an independent method claim which corresponds closely to the respective independent system claim.

VII. At the end of the oral proceedings, the chairman announced the decision of the board.

Reasons for the Decision

1. The application relates to what are called "information card systems". Such systems, in particular Microsoft's CardSpace (see the description, page 5, paragraph 2), address the problem that different "relying parties" - for instance online service providers - may impose different security policies and require different amounts of personal data from their customers (see page 4, paragraph 5). Since customers generally do not want to divulge more personal data than necessary, they

will use different "personae" vis-à-vis different relying parties. Information card systems help the user manage his multiple personae (see page 1, lines 27-32).

1.1 An information card is a data structure comprising selected personal data of a user (see e.g. figure 3).

1.2 The operation of a known information card system is depicted in figure 1: the relying party informs the user of the security policy with which he has to comply to use a requested service. The user selects a suitable information card (see also page 5, lines 15-28) - using a component aptly referred to as a card selector - and sends it to a trusted identity provider. The identity provider generates a security token, which it sends back to the user to forward to the relying party. The security token is typically encrypted or electronically signed and allows the relying party to validate the personal data and to verify that it complies with the security policy in place (page 5, line 29, to page 6, line 6).

1.3 For certain services, the cards turn out to be inconvenient. When offering a trial subscription, for instance, a service provider may want to require some sort of customer identification, so that the offer can be used only once per customer, while at the same time not deterring the customer from taking up the offer by requiring unduly sensitive data or too much of it (see page 6, last paragraph, to page 7, paragraph 1).

1.4 To address this problem, the application proposes "restricted use information cards". Such information cards additionally contain the "terms of the restriction" and the associated relying party itself. A

single card can also be used for several relying parties (see page 8, last paragraph, to page 9, paragraph 2. and figure 3, no. 305). The application further proposes that the identity provider may issue a unique "unidirectional identifier claim" to ensure that the user is not bypassing a security policy by using multiple personae or accounts (page 7, lines 11-19, and page 16, lines 11-14). The application states that the invention enables the identity provider or the relying party to track the card's usage as necessary (see sentence bridging pages 8 and 9, and page 15, lines 32-34).

1.5 The unique identifier may be generated by the identity provider based on identity information which the user need not and does not want to provide to the relying party. Therefore, the identity provider acts as an intermediary between the relying party and the user (see page 12, last paragraph, to page 13, paragraph 1). Alternatively, a broker separate from the identity provider may add the unique identifier to the security token, which is then called a brokered security token (see figure 5, and page 13, lines 9-29; see also page 15, lines 27-32).

1.6 The restricted use policy can be enforced either by the relying party or by the broker on its behalf (see page 14, lines 26-27, *et seq.*).

The prior art

2. D1 discloses an information card service of the type acknowledged as known in the application and as summarised above (see point 1.2 above, and D1, figure 7 and paragraphs 30, 31 and 57-81). D1 defines, in the context of information cards, the term "claim" as a

statement or assertion made about "the principal" (see paragraph 28) and lists amongst possible such claims (see paragraphs 38-52) the "Private Personal Identifier" (PPIDs) as "identif[ying] the subject to a relying party" (paragraph 52).

3. D5, authored by one of the inventors of D1, discusses the problems of uniquely identifying actors on the Internet, which was built without a means to do this (especially without a "native identity layer"; see page 1, first paragraphs of the "Summary" and the "Problem Statement", and the sentence bridging pages 1 and 2). D5 discloses *inter alia* the idea of using the "least identifying information" to identify an individual (e.g. his age rather than his birth date; see page 7, paragraph 7); the reuse of unique identifiers from other contexts (such as a driving licence or social security numbers; see page 7, paragraph 8), and the concept of a "unidirectional" identifier as one that is used only vis-à-vis one relying party (see page 8, paragraphs 6 and 11).

4. D6 discloses that a PPID is calculated "as a combination of the re[l]ying party certificate and something unique about [a] card" (see page 1, lines 4-5), i.e. as a unidirectional identifier in the sense of D5 (see D6, lines 12-14). It then discloses, as an improvement, setting up the system such that a "returning" user can access a service again only when he uses "the original card" obtained "during [...] registration" (see page 2, lines 18-27).

Clarity, Article 84 EPC

5. A central feature of the invention is the "unique-id claim". It is essential for solving the problem of

making returning users identifiable without forcing them to disclose sensitive private information (see the description, paragraph bridging pages 6 and 7).

6. Claim 1 of the *main* and the *(first) auxiliary request* specifies in particular that "a unique-id claim [...] provides assurances to the relying party that the user is not using multiple personas from that identity provider" and that it is "generate[d]" by the identity provider machine.

6.1 This feature implies that the relying party can assume that a user is not using multiple personae. The claims do not, however, specify what the relying party specifically does (or does not do) in view of that assurance. It is imaginable that the relying party might be willing to offer a free trial service only if provided with this assurance, but it is also possible that it might offer the free trial service either way, and merely calculate its cost differently with and without the assurance.

6.2 The claim language also leaves open how the "assurances" are "provided" by the unique-id claim, whether they are reliable, how the identity provider generates the unique-id claim and whether and how this contributes to providing the claimed assurance.

6.3 For example, if a user's unique social security number was contained in every security token, it would provide the required assurance. That users might not want to disclose their social security number (see the description, page 2, lines 20-22, and the paragraph bridging pages 6 and 7) is immaterial in this regard. Apart from the fact that different users may have different preferences, the claim language does not

define the unique-id claim in terms of what users like or dislike, nor does it specifically exclude social security numbers. Alternatively, the identity provider could simply inform the relying party that it trusts an individual customer not to use multiple personae. It is further imaginable that the identity provider might derive its trust from a mere declaration from the customer.

6.4 It is therefore unclear whether and in what way the "unique-id" that "provides assurances to the relying party" limits the claimed subject-matter, especially the feature "the identity provider machine being adapted to generate the unique-id claim", and whether the "unique-id claim" is any different from any other identifier and how.

6.5 With reference to D6, the appellant argued that the term "unique-id claim" was commonly known to the skilled person and suggested that a unique-id claim according to D6 would be understood by the skilled person as "a combination of the PPID and the public key of the token issuer" (see D6, page 2, lines 21-22 and 32-34).

6.6 The board is not convinced by this argument.

6.6.1 Firstly, it considers that the cited blog-entry is, on its own, insufficient to establish that the term "unique-id" is commonly used in the art.

6.6.2 Secondly, even if the term was in common use, D6 is insufficient to establish precisely which features the skilled person would understand to be implied by this term. In this regard, the board notes that it is not the combination of the "PPID with cryptographic

material associated with the token issuer"(D6, page 2, last paragraph, lines 3-4) that can provide the claimed "assurance" of uniqueness but, if anything, the fact that "only the use of the original card will grant access". D6, however, lacks detail as to how precisely this effect is achieved.

6.6.3 Thirdly, the board is convinced that any assurances provided by the unique-id claim are dependent on how the identity provider machine generates or (re-)produces the unique-id claim, about which claim 1 of the main and (first) auxiliary requests says nothing - irrespective of whether D6 contains any pertinent disclosure.

7. The board concludes that claim 1 of the main and the (first) auxiliary request is unclear with regard to the meaning of the term "unique-id claim" and whether and how the claimed assurances, which are essential for the subject-matter claimed, are provided by the components of the claimed system, especially the identity provider machine, and thus claim 1 does not comply with Article 84 EPC. The same conclusion applies to claims 3 of the main request and claim 4 of the (first) auxiliary request.

8. Claim 1 of the second and third auxiliary requests further specifies that the assurances are given

"... by generating the unique-id claim once, storing the unique-id claim, and using the stored claim for all subsequent requests for security tokens to the said relying party".

8.1 The board notes that this passage has been added to claim 1 at the point where it characterises the

"unique-id claim" rather than its generation, such that it might not be clear which component is meant to carry out the claimed steps of "generating", "storing" and "using". In view of the fact, however, that the identity provider machine is claimed to "generate the unique-id claim", the board takes it that the skilled person would understand that all three steps are carried out by the identity provider machine. The board also notes that the passage fails to specify the essential feature that "the stored claim" is used "for all subsequent requests" *by the same user*. In the following, the board interprets the passage above as implicitly containing this clarification.

8.2 Beyond that, however, the added passage does not specify when the identity provider generates the unique-id claim ("once") and how the user is identified so that this claim can be re-used for subsequent requests.

8.3 For the identity provider to re-issue a unique-id claim for a user, it must be able to identify that user. It seems likely that that would require some form of user registration (which is also mentioned in D6, although not disclosed in detail) and that the unique-id claim would be generated on registration (or at least between registration and the first request).

8.4 The description does not, however, mention registration, let alone disclose any details about it. The board considers that, in principle, registration might require the user to present nothing more than an email address. If so, the same person could re-register with a different email address and have a new, different "unique-id claim" generated for him. That would seem to defeat the stated purpose of the

invention (see the description, page 6, line 31, to page 7, line 3). Thus, the board also notes that the difference between a user and his personae is not clear from the claims and hence even the meaning of the claimed assurance is not clear.

8.5 The board therefore concludes that the language added to the independent claims of the second and third auxiliary requests as regards the unique-id claim fails to clarify how the unique-id claim and its generation contribute to providing the assurances claimed.

8.6 The board appreciates that the independent claims of the third auxiliary request contain additional features relating to steps carried out by the broker. Even though the description discloses that the unique-id claim can be generated by the identity provider machine or the broker, the board has doubts as to whether the description also discloses (Article 123(2) EPC) that a unique-id claim might be generated by *both* components (which may be different, see figure 5). This issue need not be decided, however, since features of the broker cannot, in themselves, clarify features of the identity provider. In passing, the board also notes that the feature of the broker relating to the unique-id claim lacks clarity for the same reasons as the corresponding feature of the identity provider.

9. In summary, the board concludes that the independent claims of all four requests on file lack clarity with regard to the "unique-id claim", Article 84 EPC.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated