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

Datasheet for the decision of 3 February 2015

Case Number:	T 0527/10 - 3.5.06
Application Number:	05100336.6
Publication Number:	1560100
IPC:	G06F1/00
Language of the proceedings:	EN

Title of invention:
Techniques for establishing and managing a distributed credential store

Applicant:
EMC Corporation

Headword:
Distributed Credential Store/EMC

Relevant legal provisions:
EPC 1973 Art. 56, 84

Keyword:
Inventive step - (no)
Claims - clarity (no)

Decisions cited:

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 0527/10 - 3.5.06

DECISION
of Technical Board of Appeal 3.5.06
of 3 February 2015

Appellant:
(Applicant)

EMC Corporation
176 South Street
Hopkinton, MA 01748 (US)

Representative:

Hanna, Peter William Derek
Hanna Moore & Curley
13 Lower Lad Lane
Dublin 2 (IE)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted on 11 November 2009 refusing European patent application No. 05100336.6 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairwoman	M.-B. Tardo-Dino
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 11 November 2009, to refuse European patent application No.05100336.6 for lack of inventive step over the document

D1: WO 99/06900 A2.

II. A notice of appeal was received on 15 December 2009, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 24 February 2010. The appellant requested that the decision under appeal be set aside and a patent be granted on the basis of claims 1-20 as filed on 18 September 2009 and as subject to the refusal, the other application documents on file being description page 2 as received on 9 April 2008, and description pages 1 and 3-18 and drawings sheets 1-3 as originally filed.

III. The board issued a summons to oral proceedings, giving in an annex its preliminary opinion that the application did not comply with Article 84 EPC 1973 and lacked an inventive step vis-à-vis document D1, Article 56 EPC 1973. Objections under Article 123 (2) EPC were also raised.

IV. In response to the summons, the appellant did not file any arguments or amendments. Instead, with a letter dated 27 January 2015, the appellant informed the board that it would not attend and be represented at the oral proceedings.

V. Oral proceedings were held as planned on 3 February 2015 in the absence of the appellant. At the end of the oral proceedings the chairwoman announced the decision of the board.

VI. Claim 1 reads as follows:

"1. A computer-implemented method, for establishing and managing a distributed credential store comprising confidential information and identity information about one or more principals and authentication techniques or services associated with authenticating the principal vis-à-vis other principals, the method comprising:

an identity service creating an initial instance of a distributed credential store when requested from a principal, the initial instance representing local credential stores, which are maintained locally on a client of the principal, and selectively linked to portions of a remote credential store, the identity service and the remote credential store are external to the client over a network, the local credential stores including credentialing records and each credentialing record having particular authentication information, particular authentication techniques, attributes that define types of the authentication information, and policies that define how the attributes are processed in a given relationship between the principal vis-à-vis another different principal, each credentialing record includes a particular relationship for interaction between the principal and one of the different principals;

a principal managing (200) the distributed credential store by:

associating (110) the portions of the remote credential store to the principal credential stores by interacting (210) with the identity service over a network, wherein the association is achieved by linking the portions of the remote credential store to corresponding portions of the principal credential stores,

using a trust specification (211, 301) that dictates a type of secure communications and methods used during interactions between the identity service and the principal,

automatically linking the linked portions over the network to the remote credential store by using means to detect interactions with the identity service once the client is detected as being connected to the network and establishes communication with the identity service over the network;

selectively synchronizing (120) changes between the portions and the principal credential stores, by using means to evaluate the trust specification to determine the selective synchronization between the portions of the enterprise credential store and the principal credential stores, and wherein the synchronization is automatically processed when the client is detected as being connected to the network; and

managing (130) conflicts and the changes with a number of the portions and the corresponding credential store during selective synchronization in response to an evaluated synchronization policy (310, 320), and wherein the synchronization effects an automatic update to the principal credential stores, the remote credential store, or to both the principal credential stores and the remote credential store;

and wherein if the principal falls out of communication with the identity service and subsequently re-establishes communication, then the identity service uses the synchronization policy communicated from the principal to generate a new active instance of the remote credential store and re-synchronize the principal's local credential stores with the identity service generated remote credential store according to the synchronization policy, and whereby the principal can maintain personal entries in the local credential stores which are not communicated to and synchronized by the identity service into the remote credential store."

The claims also comprise corresponding independent system and computer program product claims 7 and 20.

Reasons for the Decision

The appellant's absence from oral proceedings

1. The appellant was duly summoned but chose not to attend the oral proceedings. According to Article 15 (3) RPBA the board is not obliged to delay any step in the 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. The following reasons are based on the board's preliminary opinion as set out in the annex of the summons to oral proceedings to which the appellant chose not to respond in substance.

The invention

2. The application relates to a method of establishing and managing what is called a distributed credential store.

2.1 A "credential store" is described as a file, database, directory or combinations of them containing confidential information and identity information about one or more principals (p. 5, l. 21-23), where a "principal" is "an electronic representation of an entity" such as a resource, a user, an agent, an application, a system, a group, a department, [or] an object (p. 4, l. 3-6). It is disclosed that identity information as stored in the credential store may be "a legacy identification and a password pair" or "a certificate or an assertion" (p. 5, l. 27-31). The credential store may further include "authentication techniques or services" (l. 25-27) and "policies that define how attributes", which define confidential data (l. 23-25), "can or cannot be processed in a given principal-to-principal relationship" (l. 33-34).

2.2 The credential store is distributed in terms of a remote credential store (303 in fig. 3; 411 in fig. 4; also called "enterprise credential store", *e.g.* p. 9, l. 15-16) and local credential stores (302 in fig. 3; 425 in fig. 4; also called "principal credential store", *e.g.* p. 9, l. 13).

2.3 An "identity service" (410 in fig. 4) authenticates the principal and establishes a secure communication with the principal (p. 7, l. 4-6) which operates according to a "trust specification" (p. 7, l. 17-23; p. 8, l. 22-25; p. 11, l. 18-23; p. 17, l. 20-24). Secure communication typically involves encryption and signing of communication with public and private key pairs (p. 7, l. 6-10).

2.4 A local credential store is created either on request of the principal according to a "pull model" (p. 7, l. 28-29; p. 8, l. 1-2; p. 16, l. 20-22) or by the identity service or a third party according to a "push model" (p. 8, l. 2-5; p. 16, l. 22-23). Portions of the local credential store are "associated" with or "linked" to portions of the remote credential store (p. 9, l. 17-19).

2.5 The local and the remote credential stores are synchronized when changes to the credential stores are detected, according to a synchronization policy (p. 11, l. 7-16; and p. 12, l. 31 - p. 13, l. 8) which defines which portions of the local credential store are to be synchronised with which portions of the remote credential store (p. 10, l. 2-5). The principal may decide to keep some personal credential information private, *i.e.* separate from and not to be synchronised with the remote credential store (p. 10, l. 30 - p. 11, l. 5; p. 13, l. 21-28; and p. 17, l. 14-18). If communication between the principal and the identity service is interrupted for a period of time, any changes made during that period will be automatically synchronised as soon as the communication is re-established (p. 14, l. 4-13; p. 15, l. 15-23; and p. 16, l. 25-29).

Prior art

3. Document D1 discloses a method of managing the synchronisation of so-called "workspace data" (p. 3, l. 14-16; 163 and 180 in fig. 1) of a roaming user in a client-server system ("clients" 165 and 167 in fig. 1; "global server" 115 in figure 1).

3.1 Workspace data may include, for instance, e-mail or calendar data, bookmarks or "other types of data such as application programs" (p. 10, l. 14-18; p. 18, l. 17 – p. 19, l. 5). The description refers to "portions of [...] workstation data" being synchronised, copies of which are "independently modifiable" (p. 3, l. 15-16; p. 6, l. 12-14; p. 11, l. 22 – p. 12, l. 1).

3.2 The copies of the workspace data on clients and server are not necessarily identical: A user may prefer to store certain confidential or private information or part of it on the client and not on the server and *vice versa* (p. 6, l. 4-9; p. 7, l. 7-10).

3.3 The server maintains the workspace data in a so-called "global format", whereas clients may use different local formats. The translation between the different formats is performed by a so-called "global translator" (150 in fig. 1; p. 11, l. 4-6; p. 12, l. 6-12; p. 18, l. 17 – p. 19, l. 1).

3.4 The synchronisation may be initiated by the "synchronisation-start module" of a client (820 in fig. 8; p. 5, l. 1-4; p. 6, l. 14-15) and according to predetermined criteria such as upon user request, after a predetermined number of changes or after a user action such as user log-off (p. 6, l. 14-18; p. 22, l. 3-8). The synchronisation-start module instructs a "general synchronisation module" (825 in fig. 8; p. 22, l. 8-10) to begin the synchronisation. This module requests version information from the synchronisation agent of the server (145 in fig. 1), compares the remote and local versions and performs the appropriate synchronisation (p. 22, l. 14 – p. 23, l. 1). If conflicts occur, reconciliation may be needed (see p. 23, l. 1-4; p. 23, l. 13 - p. 24, l. 2; and 830 in fig. 8).

Clarity, Article 84 EPC 1973

4. The board considers the independent claims to be unclear in a number of respects, Article 84 EPC 1973.

4.1 Independent claims 1 and 7 specify that the "local credential stores are selectively linked to portions of a remote credential store". The board considers unclear the meaning of "selective linking" and the suggestion that entire "stores" are linked to "portions", Article 84 EPC 1973. In view of the description the board considers the intended meaning of that phrase to be that data stores are "linked" so that corresponding portions can be identified and set up so that selective synchronisation is possible, *i.e.* so that some portions of the remote credential store are subject to synchronisation, whereas some portions of it are not.

4.2 Claim 1 specifies that a principal "associates the portions of the remote credential store to the principal credential store, wherein the association is achieved by linking the portions". In the board's view the difference between "associating" and "linking" portions of credential stores is unclear.

4.3 Claim 1 comprises a further step of "automatically linking the linked portions" although the portions should have already been linked in the course of "associating the portions". This apparent redundancy also renders the claim unclear.

4.4 Independent claims 1 and 7 both specify that "each credentialing record includes a particular relationship for interaction between the principal and one of the different principals" (last sentence of the first method step in claim 1; last sentence of "a principal service (420) ... " in claim 7). The board considers this wording to be unclear. While it is typical for credentials to make reference to - *i.e.* "include" - relationships between principals such as the owner of a credential, the issuing entity and the object to which the credential relates, it is unclear what is meant by the relationship being "for interaction". Moreover, the board considers this feature to be redundant over the feature directly preceding it in the claim which requires each "credentialing record [to] hav[e] policies that define how attributes are processed in a given relationship between the principal vis-à-vis another different principal".

Inventive Step, Article 56 EPC 1973

5. Despite the clarity issues raised above the board deems it appropriate in the present case to give its assessment of inventive step as well.

6. The examining division considered D1 to disclose that "workspace data also comprises credentials, *e.g.* keys and digital certificates" (see decision under appeal, p. 2, last line), based on a short passage in D1 mentioning some sort of synchronisation of credentials (p. 7, l. 21 - p. 8, l. 5). The appellant challenged this finding of the decision, arguing that "workspace data" according to D1 was "essentially user-created data", as was illustrated on page 10, lines 14-18, and thus did not comprise credential information (grounds of appeal, point 2.6). Instead, so the appellant's argument, all credential information in D1 was stored in keysafe 365 at the global server (fig. 3; see grounds of appeal, point 2.3).

6.1 Although the board does not regard the examining division's interpretation of D1 to be unreasonable, it considers any speculation as to whether the "workspace data" in D1 comprises credentials immaterial to the conclusion that the claimed invention lacks an inventive step. In particular, the present invention is not concerned with any characteristic of credential information which provides for improved security. Credential information of the invention is merely the object of a data synchronisation method. The board considers the type of the synchronised data being of a particular type, *i.e.* credentialing records, not to necessitate the solution of a technical problem. The board further does not consider any speculation on the "keysafe 365" of D1 to be relevant.

6.2 The appellant emphasises several times in the grounds of appeal that the invention is more than mere data synchronization. As the credential records also defined "a given relationship of interaction between one principal vis-à-vis other principals", the invention provided for synchronisation of relationships whereas D1 did not (see grounds of appeal, points 2.9 and 2.12). In view of the above (see point 4.4 *supra*), the significance given by the appellant to the term "relationship" is not apparent to the board. Thus the board takes the appellant's considerations in this regard not to go beyond its argument mentioned above that the synchronised data in D1 does not include credentials.

6.3 The decision under appeal (reasons 2.3) considered claim 1 to differ from D1 in the use of a trust specification dictating a type of secure communication between the identity service and the principal. The board does not concede this difference, rather considering that D1 discloses that the clients and the server communicate in a secure manner and according to multiple levels of access based on the level of identification and authentication (p. 11, l. 11-15; p. 16, l.

14 - p. 17, l. 7). In the board's view, the skilled person would consider this to constitute a "trust specification".

6.4 In its grounds of appeal, the appellant argues that D1 is different from the claimed invention in a number of ways, in particular it alleges that D1 described a centralized system managed from the server side whereas the present invention related to "distributed systems, managed locally from the client side" (see grounds of appeal, points 2.4 and 2.5), that D1 did not disclose the linking of portions of the client and server data (see grounds of appeal, points 3.2 and 3.3), and that D1 did not disclose personal entries in the local store (see grounds of appeal, point 3.6). The board disagrees. D1 indeed discloses a distributed client-server architecture (115, 165, 167 in fig. 1). Some "linking" between portions of data stores, broadly construed in view of the clarity objections above (see points 4.1-4.3 *supra*), is a prerequisite for any data synchronisation. And D1 discloses the possibility to exclude personal data from synchronisation (p. 7, l. 5-10).

7. Therefore the board considers the subject matter of claim 1 to differ from D1 by the following features:

i) D1 does not disclose that the local instance of the data store is initially created on the client's request.

ii) The synchronised data in D1 does not include credentialing records with the particular information content as claimed.

iii) D1 does not disclose that a client and the server are re-synchronised when they fall out of communication and re-establish communication.

Differences i), ii) and iii) broadly correspond to the differences 2.1), 2.2) and 2.4) as identified in the decision under appeal (p. 4-5).

7.1 The board considers that the problems addressed by these differences do not interact with each other in any non-trivial manner and that, hence, their respective inventive merit may be considered independently.

7.2 *Re. difference i),* it would be obvious to the skilled person to create an initial instance of a data store at the request of the client. If the "roaming user" of D1 (p. 1, l. 17 -24) starts working on a particular client (p. 6, l. 12-14) and wants to resume a task that was interrupted before at another client, the new client will have to have the pertinent workspace data downloaded from the global server to initiate a local copy at the new client.

7.3 *Re. difference ii),* the skilled person would not need to solve any technical problem in applying the teachings of D1 to the synchronisation of any particular kind of data such as the credential records of claim 1 (see also point 6.1 *supra*).

7.4 *Re. difference iii),* the board considers synchronisation frequency to be a common design decision of a distributed database such as the claimed one. The skilled person would balance the need for synchronicity and accuracy against the communication costs involved according to circumstances and as a matter of routine without exercising any inventive activity.

7.5 Therefore, the board comes to the conclusion that the independent claims 1, 7 and 20 are not inventive over D1 in the sense of Article 56 EPC 1973.

7.6 It follows from the above that the appeal has to be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairwoman:

Beschwerdekammern des Europäischen Patentamts
Boards of Appeal of the European Patent Office
Chambres de recours de l'Office européen des brevets

B. Atienza Vivancos M.-B. Tardo-Dino

Decision electronically authenticated