BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS | **BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE** | **CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN 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 24 July 2012

Case Number:	T 1597/08 - 3.5.05
Application Number:	04027129.8
Publication Number:	1505473
IPC:	G06F 1/00
Language of the proceedings:	EN

Title of invention:
Methods and arrangements for mapping widely disparate portable tokens to a static machine concentric cryptographic environment

Applicant:
MICROSOFT CORPORATION

Headword:
Interfacing tokens to cryptographic machine/MICROSOFT

Relevant legal provisions (EPC 1973):
EPC Art. 54, 56, 83, 84

Keyword:
"Oral proceedings held in the absence of the appellant"
"Clarity and sufficiency of disclosure - yes"
"Main request and first auxiliary request - Novelty (no)"
"Second and third auxiliary requests - Inventive step (no)"

Decisions cited:
-

Catchword:
-

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

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1597/08 **-** 3.5.05

DECISION
of the Technical Board of Appeal 3.5.05
of 24 July 2012

Appellant:
(Applicant)

MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052 (US)

Representative:

Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Leopoldstrasse 4
D-80802 München (DE)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted 27 February 2008 refusing European patent application No. 04027129.8 pursuant to Article 97(2) EPC.

Composition of the Board:

Chair: A. Ritzka
Members: P. Cretaine
G. Weiss

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division to refuse European patent application No. 04 027 129.8, published as EP 1 505 473. The decision was announced in oral proceedings held on 9 November 2007 and written reasons were dispatched on 27 February 2008.

II. The application was refused because claim 1 of a main request and claim 1 of a first auxiliary request were not supported by the description (Article 84 EPC 1973) and because of lack of disclosure of the invention according to the main and first auxiliary requests (Article 83 EPC 1973). The application was further refused because the subject-matter of claim 1 according to the second and third auxiliary requests lacked inventive step, having regard to the disclosure of

D1: Interoperability Specification for ICCs and Personal Computer Systems, Parts 1 to 8, Revision 1.0, December 1997.

III. The notice of appeal was submitted on 8 May 2008 and the appeal fee was paid on the same day. In the notice of appeal, the appellant (applicant) requested that the decision under appeal be set aside and a patent be granted on the basis of the claims, description and drawings on file. In the statement setting out the grounds of appeal, submitted on 2 July 2008, the appellant referred to the main and auxiliary requests as attached to the decision under appeal. Therefore the board assumed that the appellant had requested the grant of a patent based on one of the set of claims refused in examination proceedings. The appellant also requested oral proceedings on an auxiliary basis.

IV. A summons to oral proceedings to be held on 24 July 2012 was issued on 20 April 2012. In an annex accompanying the summons, the board expressed the preliminary opinion that the main and first auxiliary requests met the requirements of Articles 83 and 84 EPC 1973. However the board expressed the view that the subject-matter of claim 1 according to the main and first auxiliary requests was not new (Article 54 EPC 1973) and that the subject-matter of claim 1 according to the second and third auxiliary request did not involve an inventive step (Article 56 EPC 1973), having regard to the disclosure of D1.

V. With a letter received on 31 May 2012, the appellant informed the board that he would not be attending the scheduled oral proceedings and withdrew his request for oral proceedings. The appellant did not submit any comments as to the substance of the board's objections.

VI. The appellant requested in writing that the decision under appeal be set aside and that a patent be granted on the basis of the claims 1 to 10 filed by letter of 10 March 2006 (main request) or in the alternative on the basis of claims 1 to 10 filed as first, second and third auxiliary requests during the oral proceedings before the examining division on 9 November 2007.

VII. Oral proceedings were held as scheduled on 24 July 2012 in the absence of the appellant who had been duly summoned. After deliberation on the basis of the written submissions, the chair announced the board's decision at the end of the oral proceedings.

VIII. Independent claim 1 of the main request reads as follows:

"An interface method that permits the use of widely disparate portable tokens (202) in a static machine concentric environment, the interface method comprising:
for each one of said widely disparate portable tokens, instantiating a single card control object (302) that is operatively configured to manage the portable token;
from the card control object, instantiating at least one container control object (308) that is configured to manage a specific key container; and
from the container control object, instantiating at least one key pair control object (314) that is configured to manage at least one individual key pair maintained on the portable token."

Independent claim 1 according to the first auxiliary request reads as follows:

"An interface method that permits the use of widely disparate portable tokens (202) in a static machine concentric cryptographic environment in support of, or for completion of, cryptographic functions, the interface method comprising:
for each one of said widely disparate portable tokens, instantiating a single card control object (302) that is operatively configured to manage the portable token;
from the card control object instantiating at least one container control object (308) that is configured to manage a specific key container; and

from the container control object, instantiating at least one key pair control object (314) that is configured to manage at least one individual cryptographic key pair maintained on the portable token."

Independent claim 1 according to the second auxiliary request reads as follows:

"An interface method of using a plurality of widely disparate portable tokens (202) in a static machine concentric environment, said plurality being a magnetic disk, an optical disk and a smart card, the interface method comprising:
for each one of said widely disparate portable tokens, instantiating a single card control object (302) that is operatively configured to manage the portable token;
from the card control object, instantiating at least one container control object (308) that is configured to manage a specific key container; and
from the container control object, instantiating at least one key pair control object (314) that is configured to manage at least one individual key pair maintained on the portable token."

Independent claim 1 according to the third auxiliary request reads as follows:

"An interface method of using a plurality of widely disparate portable tokens (202) in a static machine concentric environment said plurality being a magnetic disk, an optical disk and a smart card, the interface method comprising:

for each one of said widely disparate portable tokens, instantiating a single card control object (302) that is operatively configured to manage the portable token;
from the card control object, instantiating at least one container control object (308) that is configured to manage a specific key container;
from the container control object, instantiating at least one key pair control object (314) that is configured to manage at least one individual key pair maintained on the portable token; and
from at least one control object selected from a set comprising the card control object, the at least one container control object, and the at least one key pair control object, instantiating a certificate list object (304, 310, 316) that is configured to enumerate over a set of certificate objects (306, 312, 318) associated with said at least one control object."

Reasons for the Decision

1. The appeal is admissible.

2. *Non-attendance at oral proceedings*

The appellant was duly summoned, but did not 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, on the grounds that some party duly summoned to the oral proceedings is absent, that party then being treated as relying solely on its written case. In the present case, the board was in a position to take a decision at the end of the hearing.

3. *Clarity of claims and sufficiency of disclosure of the claimed invention*

The decision under appeal stated that the portable token defined in claim 1 according to the main request could be read onto a bus ticket; as a consequence claim 1 was not supported by the description, and the way that the claimed method could be applied to a bus ticket was not disclosed in the application.

Although a link may exist between the serial and customer numbers inscribed on a bus ticket, these two numbers cannot be considered, in the board's judgment, as a key pair maintained on a token. The feature in claim 1 that the "key pair" is "maintained on the portable token" is an unambiguous, although implicit, reference to the field of cryptography. Therefore, the "key pair" mentioned in claim 1 is to be considered by the skilled person as a cryptographic key pair, the two keys being linked by their potential use in the same cryptographic algorithm. There is no evidence and it seems highly improbable that the serial and customer numbers on a bus ticket represent a cryptographic key pair. There is therefore no lack of disclosure in the application documents according to the main request as to how the claimed method can be applied to a bus ticket.

Moreover, in the light of the description, which clearly refers to the field of cryptography (see paragraph [0002] of the published application), and taking into account the common general knowledge in that field, claim 1 does not lack clarity with respect to the definition of a portable token used in a machine and maintaining a key pair.

This reasoning also applies to claim 1 according to the first auxiliary request, all the more since the static machine concentric environment in which the token is used and the key pair are explicitly qualified as, respectively, static machine concentric **cryptographic** environment and **cryptographic** key pair.

The board therefore judges that claim 1 of the main and first auxiliary requests meets the requirements of Article 84 EPC 1973 and that the application according to the main and first auxiliary requests meets the requirements of Article 83 EPC 1973.

4. *Novelty and inventive step*

4.1 Prior art

D1 is an interoperability specification for ICCs and a personal computer system comprising an operating system (see part 1, point 2.3). The system architecture disclosed therein comprises (see in particular part 1, figures 2-1 and 2-3):

- integrated circuit cards (ICCs), e.g. smart cards, exposing cryptographic functionalities;

- interface devices (IFDs) as physical interface devices (e.g. smart card readers) between the personal computer system and the ICCs;

- interface device handlers (IFD handlers) for mapping the capabilities of the IFDs to the personal computer system;

- an ICC resource manager for supporting controlled access to IFDs and through them, individual ICCs;

- a service provider for encapsulating functionalities exposed by a specific ICC and making them accessible to the personal computer system through high-level programming interfaces and comprising a cryptographic service provider for specifically accessing ICC cryptographic functionalities (see part 1, points 2.1.5 and 2.1.5.2).

- an ICC-aware application which wants to make use, through the service provider of the computer system, of the functionalities provided by the ICCs.

4.2 Main request

The board considers that the "widely disparate portable tokens" defined in claim 1 can be read onto the ICCs of D1. The appellant argued that the detailed requirement specifications (e.g. dimensions, locations of contacts, voltage and current conditions) set out in D1, Part 2., restricted the use of the interface method of D1 to a specific portable token. The board is not convinced by this argument since the card specifications of D1 do not define a single specific card but rather a whole class of cards which therefore fall under the broad and vague definition of "widely disparate portable tokens".

Moreover, D1 discloses (see Part 6., points 2.2 and 2.5) that an ICC resource manager makes accessible the cryptographic information stored in the ICC to the ICC-aware application through the service provider. This is achieved (see Part 1, points 2.1.5 and 2.1.5.1; Part 6, points 2.2 and 3.3.1; Figure 3.1) by the service provider abstracting implementation details at ICC level and exposing them in a standard way that the application software can easily access, using interfaces which may be implemented using object-oriented languages. In particular the instantiation, for each connected ICC, of a SCARD object (see Part 6, point 3.3.1 in combination with Figure 3.1), the instantiation of a CRYPTPROV object (see Part 6, point 3.4.4 in combination with Figure 3.1) and the instantiation of a CRYPTKEY object (see Part 6, point 3.4.6 in combination with Figure 3.1) amount, in the board's view, to instantiating a single card control object, a container control object, and a key pair control object, respectively, as defined in claim 1.

The board further notes that the appellant has not rebutted the argumentation of the examining division, set out in point 14.1 of the Reasons for the decision, that the object hierarchy defined in the application is already known from D1.

Thus, the board holds that the subject-matter of claim 1 is already known from D1 (Article 54 EPC 1973).

4.3 First auxiliary request

Claim 1 adds to claim 1 according to the main request that the static machine concentric environment is for cryptographic functions and that the key pair is a cryptographic key pair. Since both features are disclosed in D1 (see in particular part 1, point 2.1.5.2), claim 1 does not meet the requirements of Article 54 EPC 1973 for the reasons mentioned in point 4.2 above in respect of claim 1 of the main request.

4.4 Second auxiliary request

Claim 1 adds to claim 1 according to the main request that the tokens are magnetic disks, optical disks or smart cards.

The steps of the claimed method do not however rely on the nature of the token (smart card, optical or magnetic disk) but on the cryptographic information or function stored in the token. The added feature does not therefore combine with the method steps to provide any surprising technical effect. The skilled person, being aware of the storing capabilities of magnetic and optical disks, would implement the interface method of D1 in a system comprising magnetic and optical disks as tokens without requiring any inventive skill. For these reasons the board holds that the subject-matter of claim 1 does not involve an inventive step (Article 56 EPC 1973), having regard to the disclosure of D1.

4.5 Third auxiliary request

Claim 1 adds substantially to claim 1 according to the second auxiliary request the feature of instantiating from a control objet being either the card control object, the container control object, or the key pair control object, a certificate list object configured to enumerate a set of certificate objects associated with the control object. D1 teaches the use of public key cryptography for authentication and digital signatures services provided by an ICC (see Part 8, points 2 and 3), based on the key pair (public and private keys) stored in the ICC. It is common practice in public key cryptography schemes to maintain a list of valid digital certificates containing certified public keys. In order to implement the public key cryptography functionalities provided by an ICC (or portable token) in D1, the skilled person would need to use valid public keys and would thus maintain a certificate list for this portable token. To do this, the skilled person would consider instantiating an object, a certificate list object, in the same manner as objects have been instantiated in the object hierarchy of D1 for managing the portable token, its key containers and its key pairs. The choice of the hierarchy level at which the certificate list object should be instantiated (card control object, container control object, or key pair control object) lies within the general design competence of the skilled person.

For these reasons the board holds that the subject-matter of claim 1 does not involve an inventive step, having regard to the disclosure of D1.

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

Order

For these reasons, it is decided that:

The appeal is dismissed.

The Registrar: The Chair:

K. Götz A. Ritzka