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 20 July 2010

Case Number: T 1318/06 - 3.5.05

Application Number: 00945066.9

Publication Number: 1203276

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:
Cryptographic computer interface for smart cards/MICROSOFT

Relevant legal provisions (EPC 1973):
EPC Art. 56, 106, 107, 108

Keyword:
"Main request - inventive step (no)"
"First auxiliary request - inventive step (no, after amendment)"
"Second auxiliary request - inventive step (no, after amendment)"

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1318/06 - 3.5.05

D E C I S I O N
of the Technical Board of Appeal 3.5.05
of 20 July 2010

Appellant: MICROSOFT CORPORATION
One Microsoft Way
Redmond
WA 98052 (US)

Representative: Eickelkamp, Thomas
Grünecker, Kinkeldey
Stockmair & Schwanhäusser
Anwaltssozietät
Leopoldstrasse 4
D-80802 München (DE)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 7 March 2006 refusing European patent application No. 00945066.9 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

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

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division announced in oral proceedings held on 2 February 2006, with reasons dispatched on 7 March 2006, refusing European patent application No. 00 945 066.9 on the grounds that the independent claims 1 and 50 did not meet the requirements of Article 54(1) and (2) EPC 1973 since their subject-matter was known from the following prior art document:

D2: "Interoperability Specification for ICCs and Personal Computer Systems", Dec, 1997, http://www.pcscworkgroup.com/specifications/specdownload V1.php.

II. The notice of appeal was dated and received 17 May 2006. The appeal fee was paid on the same day. It was requested that the decision to refuse be cancelled. The grant of a patent was requested on the basis of the set of claims (main request) filed on 2 January 2006 and on which the appealed decision had been based. A precautionary request for oral proceedings was also made. With the statement setting out the grounds of appeal dated and received 17 July 2006, the appellant filed claims of a first and a second auxiliary requests.

III. In a communication accompanying a summons to oral proceedings to be held on 23 July 2010, the board gave a preliminary opinion that the independent claims according to the main and first auxiliary requests did not involve an inventive step having regard to the combination of D2 with the following additional prior art document referred to by the board:

D3: US 5 689 565 (D3 is a patent document assigned to the appellant. It was cited in the application).

With respect to the second auxiliary request, the board presented objections under Article 84 EPC 1973. Without prejudice to these objections, the board was of the preliminary opinion that the independent claims of the request were not allowable due to lack of inventive step (Article 56 EPC 1973).

IV. With a letter of reply dated 23 June 2010 and received at the EPO on the same date, the appellant informed the board that he would not attend the oral proceedings and that he withdrew his request for oral proceedings. The appellant also requested that a decision according to the state of the file (sic) be issued.

No submissions or amendments in response to the issues raised by the board were received.

V. In a short communication issued on 29 June 2010, the board informed the appellant that the oral proceedings were cancelled.

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

"An arrangement for use with a machine (130, 178), the arrangement comprising:
an operating system (158);
at least one application programming interface (240) that is configured to provide an interface between application programs and a plurality of cryptographic server provider functions; and

at least one cryptographic server provider (244, 246), characterized in that
the machine has the capability to operatively couple with at least one removable portable token device (200, 202, 206),
the at least one application programming interface is included in the operating system,
the at least one cryptographic server provider is a portable token cryptographic server provider included in the operating system and operatively configured to provide an interface between the application programming interlace and the portable token; and
the arrangement further comprises at least one portable token service provider (248) that is operatively configured to use the portable token cryptographic server provider to create an object-based information interface (300) to unique cryptographic information maintained within the portable token."

Independent claim 50 of the main request reads as follows:

"A method for use with a machine, the method comprising:
providing an operating system (158);
providing at least one application programming interface (240) configured to provide an interface between application programs and a plurality of cryptographic server provider functions; and
providing at least one cryptographic server provider (244, 246),
characterized in that
the method is for use with a machine having the capability to operatively couple with at least one removable portable token device (200, 202, 206),

the at least one application programming interface is included in the operating system,
the at least one cryptographic server provider is a portable token cryptographic server provider included in the operating system and operatively configured to provide an interface between the application programming interface and the portable token, and
the method further comprises:
providing at least one portable token service provider (248) that is operatively configured to use the portable token cryptographic server provider to create an object-based information interface (300) to unique cryptographic information maintained within the portable token."

Claim 1 of the first auxiliary request reads as follows:

An arrangement for use with a machine (130, 178), the arrangement comprising:
an operating system (158);
at least one application programming interface (240) that is configured to provide an interface between application programs and a plurality of cryptographic server provider functions; and
at least one cryptographic server provider (244, 246), characterized in that
the machine has the capability to operatively couple with at least one removable portable token device (200, 202, 206),
the at least one application programming interface is included in the operating system,
the at least one cryptographic server provider is a portable token cryptographic server provider included in the operating system and operatively configured to

provide an interface between the application programming interface and the portable token; and
the arrangement further comprises at least one portable token service provider (248) not included in the operating system and operatively configured to use the portable token cryptographic server provider to create an object-based information interface (300) to unique cryptographic information maintained within the portable token,
wherein the at least one application programming interface (240) is configured to contact said at least one cryptographic server provider (244, 246) that is configured to work with a portable token service provider (248), in response to a request from an application for a cryptographic function, wherein the cryptographic server provider (244, 246) is configured to look up the portable token service provider (248), and wherein the requested cryptographic function is provided to the requesting application."

Independent claim 50 of the first auxiliary request reads as follows:

"A method for use with a machine, the method comprising:
providing an operating system (158);
providing at least one application programming interface (240) configured to provide an interface between application programs and a plurality of cryptographic server provider functions; and
providing at least one cryptographic server provider (244, 246),
characterized in that

the method is for use with a machine having the capability to operatively couple with at least one removable portable token device (200, 202, 206),
the at least one application programming interface is included in the operating system,
the at least one cryptographic server provider is a portable token cryptographic server provider included in the operating system and operatively configured to provide an interface between the application programming interface and the portable token, and
the method further comprises:
providing at least one portable token service provider (248) not included in the operating system and operatively configured to use the portable token cryptographic server provider to create an object-based information interface (300) to unique cryptographic information maintained within the portable token,
wherein the method further comprises:
an application program requesting a cryptographic function from the at least one application programming interface (240),
the at least one application programming interface (240) contacting the at least one cryptographic server provider (244, 246) that is configured to work with a portable token service provider (248),
the cryptographic server provider (244, 246) looking up the portable token service provider (248), and
the requested cryptographic function is provided to the requesting application program."

Claim 1 of the second auxiliary request reads as follows:

"An arrangement for use with a machine (130, 178), the arrangement comprising:
an operating system (158);
at least one application programming interface (240) that is configured to provide an interface between application programs and a plurality of cryptographic server provider functions; and
at least one cryptographic server provider (244, 246), characterized in that
the machine has the capability to operatively couple with at least one removable portable token device (200, 202, 206),
the at least one application programming interface is included in the operating system,
the at least one cryptographic server provider is a portable token cryptographic server provider included in the operating system and operatively configured to provide an interface between the application programming interface and the portable token,
the arrangement further comprises at least one portable token service provider (248) that is operatively configured to use the portable token cryptographic server provider to create an object-based information interface (300) to unique cryptographic information maintained within the portable token,
the portable token service provider (248) includes a base object that is never instantiated by itself, but defines attribute management services among a plurality of other portable token service provider interfaces,
the portable token service provider (248) further includes a control object that inherits from the base object, but defines a plurality of common services that can be used among differing control interfaces associated with the portable token service provider,

the portable token service provider (248) further includes a container control object interface that inherits from the control object and provides access to individual key pairs within an identified container within the portable token,
the portable token service provider (248) further includes a key pair control object interface that inherits from the control object and is configured to provide selective access to the services of an identified key pair within the portable token, and
the portable token service provider (248) further includes a certificate object interface that inherits from the base object and is configured to identify a specific digital certificate within a certificate list."

Independent claim 45 of the second auxiliary request reads as follows:

" A method for use with a machine, the method comprising:
providing an operating system (158);
providing at least one application programming interface (240) configured to provide an interface between application programs and a plurality of cryptographic server provider functions; and
providing at least one cryptographic server provider (244, 246),
characterized in that
the method is for use with a machine having the capability to operatively couple with at least one removable portable token device (200, 202, 206),
the at least one application programming interface is included in the operating system,

the at least one cryptographic server provider is a portable token cryptographic server provider included in the operating system and operatively configured to provide an interface between the application programming interface and the portable token,
the method further comprises providing at least one portable token service provider (248) that is operatively configured to use the portable token cryptographic server provider to create an object-based information interface (300) to unique cryptographic information maintained within the portable token,
the portable token service provider (248) includes a base object that is never instantiated by itself, but defines attribute management services among a plurality of other portable token service provider interfaces,
the portable token service provider (248) further includes a control object that inherits from the base object, but defines a plurality of common services that can be used among differing control interfaces associated with the portable token service provider,
the portable token service provider (248) further includes a container control object interface that inherits from the control object and provides access to individual key pairs within an identified container within the portable token,
the portable token service provider (248) further includes a key pair control object interface that inherits from the control object and is configured to provide selective access to the services of an identified key pair within the portable token, and
the portable token service provider (248) further includes a certificate object interface that inherits from the base object and is configured to identify a

specific digital certificate within a certificate list."

Reasons for the Decision

1. *Admissibility*

The appeal complies with the provisions of Articles 106 to 108 EPC 1973 (see Facts and Submissions, point II). Therefore it is admissible.

2. *Novelty and inventive step*

2.1 Closest prior art

D2 is an interoperability specification for ICCs and personal computer systems. The system architecture comprises (see in particular D2, part 1, figures 2-1 and 2-3):

– integrated circuit cards ICCs (e.g. smart cards);

– interface devices IFDs as physical interface devices (e.g. smart card readers) for the ICCs;

– interface device handlers (IFD handlers) for mapping the capabilities of the IFDs to the 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 computer system through high-level programming interfaces and comprising a Cryptographic Service Provider for specifically accessing ICC cryptographic functionalities;

– an ICC-Aware application which wants to make use, through the Service Provider of the computer system, of the functionalities provided by the ICCs.

2.2 Main request:

2.2.1 The board considers the following features of claim 1 to be disclosed by D2:

– the operating system can be read onto the operating system of the PC in D2 (see part 1, point 2.3);

– the "high-level programming interfaces" disclosed in D2, part 1, points 2.1.5 and 2.1.5.2, which teaches that the service provider makes the ICC cryptographic functionality accessible through these high-level programming interfaces, correspond to the application programming interface API;

– the removable portable token device can be read onto an ICC exposing cryptographic functionalities in D2;

– the cryptographic server provider is disclosed as "cryptographic service provider" in D2, part 1, 2.1.5.2;

– the portable token service provider can be read onto the ICC resource manager in D2: In this respect, part 6, points 2.2 and 2.5, discloses that the ICC resource manager makes accessible the cryptographic information stored in the ICC to the ICC-Aware application through the service provider. Moreover part 6, point 2.2, discloses that the service provider abstracts implementation details at the ICC level and exposes them in a standard way that application software can easily access, using interfaces which may be implemented using object-oriented languages. Therefore the board judges that D2 discloses, using the wording of claim 1, a portable token service provider (ICC resource manager in D2) configured to use the portable token cryptographic server provider (cryptographic service provider in D2) to create an object-based information interface to unique cryptographic information maintained within the portable token (ICC in D2).

2.2.2 The appellant argued that the line in figure 2-3 in part 1, point 2.2 of document D2 between the Application block and the Service Provider block may represent an interface but not an application programming interface, as stated by the examining division in the refusal decision. This argument does not convince the board as the first paragraph in part 1, point 2.1.5, unambiguously discloses the provision of application programming interfaces through which the

service provider makes the ICC functionalities accessible to the applications.

The appellant further argued that D2 does not disclose that the ICC resource manager **uses** the cryptographic service provider to **create** an object-based information interface to the information within an ICC. Since claim 1 does not specify how the object-based information interface is created but merely states in substance that it is created by an interaction between the portable token service provider and the portable token cryptographic server provider, the board considers that such an interaction is disclosed in D2, namely due to the fact that the cryptographic service provider accesses the cryptographic information within the ICC through the ICC resource manager.

D2 does not unambiguously disclose that the application programming interface (API) and the ICC cryptographic service provider are "included in the operating system". Thus, the board judges this feature to be the only distinguishing feature between the subject-matter of claim 1 and the disclosure of D2.

The wording "included in the operating system" may be interpreted in several ways: it could mean, inter alia, "sold with the operating system package", or "issued by the operating system supplier", or "running at the same priority/session level as the kernel", or "developed and supplied by the vendor of the operating system".

Figure 3 of the application shows that the functional blocks corresponding to the API (240) and the portable token cryptographic server provider (246) belong to the

functional block corresponding to the operating system (158), whereas the functional block corresponding to the portable token service provider (248) does not. Moreover the passage on page 17, lines 9-13 describes that the portable token service provider is developed/supplied by the smart card vendor. The board therefore judges that the wording "included in the operating system" has to be interpreted, in the light of the description and drawings, as meaning developed and supplied by the vendor of the operating system.

This interpretation is also used by the appellant who based his argumentation that the application programming interface and the cryptographic service provider in D2 are not "included in the operating system" on passages of D2 which disclose that the service provider is intended to be developed as a user-mode application module (part 6, point 2.7) and that the application programming interface might be expected to come from sources different than the operating system issuer (part 6, point 2.1).

2.2.3 The technical effects of having the application programming interface (API) and the portable token cryptographic server provider (CS-CSP) developed and supplied by the operating system issuer have not been addressed by the appellant in his statement setting out the grounds of appeal. In the board's view, this enables the operating system issuer instead of the smart card supplier to get more control and trust in the API and the CS-CSP. The objective technical problem is thus seen as how to provide an alternative to the repartition of tasks between operating system issuer

and smart card issuer for implementing the API and CS-CSP.

The skilled person would first note that D2 does not explicitly preclude the application programming interface and the cryptographic service provider to be developed by the operating system issuer. Looking for an alternative, he would further consult document D3, which lies in the same technological field of a cryptography system using a smart card. D3 discloses cryptography system architecture (see figure 10) for making the cryptographic information stored in a card accessible to application program, for instance for making the authentication information stored in a credit card accessible to an electronic commerce application. The cryptographic system comprises an application programming interface (CAPI 172 in figure 10) and a cryptographic server provider (CSP 174 in figure 10). D3 teaches at column 17, lines 8-12 that, as an alternative, the cryptographic system could be incorporated into an operating system, which means that the application programming interface and the cryptographic server provider could be included in the operating system within the meaning defined in paragraph 2.2.2 above. The skilled person would thus implement this feature of D3 in the architecture of D2 without the exercise of any inventive skill, thereby arriving at the subject-matter of claim 1.

Claim 1 therefore does not meet the requirements of Article 56 EPC 1973.

Independent claim 50 contains the same features as claim 1 but expressed in the terms of a method claim.

Claim 50 therefore does not meet the requirements of Article 56 EPC 1973.

2.3 First auxiliary request

The features that this request adds to the independent claims of the main request are the following:

a) the portable token service provider (SCCP) is not included in the operating system;

b) the application programming interface contacts the cryptographic server provider that is configured to work with a portable token service provider, in response to a request from an application for a cryptographic function, wherein the cryptographic server provider looks up the portable token service provider and wherein the requested cryptographic function is provided to the requesting application.

As to feature a), the board notes that, although D2 suggests to have the ICC Resource Manager "provided by the operating system vendor" (part 5, point 2.1), it does not preclude the system designer from having it developed/supplied by an other source. Since the appellant did not mention any technical effect provided by this feature, the board judges that it represents an obvious alternative for the skilled person with no inventive merit in itself.

As to feature b), the board judges that, since it defines in broad and vague terms ("request", "contacts", "look-up") the interactions between the functional blocks (API, SC-CSP, SCCP and SC) of the system, it is

implicitly disclosed in D2, which relates to a similar system architecture (see D2, part 1, figure 2.1, and paragraph 2.2 above). In particular, D2, part 6, points 2.1, 2.4 and 2.5, disclose that the cryptographic service provider is the mechanism through which an application can access cryptographic data or services on a specific ICC by using an application programming interface exposed to the application. The application programming interface therefore is the interface between the requesting application and the cryptographic service provider, which in turn is connected to the ICC resource manager. Therefore, the interactions defined in feature b) are disclosed in D2, merely as a logical consequence of the functional blocks arrangement disclosed therein.

Moreover, features a) and b) do not combine to provide any surprising technical effect but only represent juxtaposed features in the independent claims of the first auxiliary request.

For these reasons, the independent claims of the first auxiliary request do not meet the requirements of Article 56 EPC 1973.

2.4 Second auxiliary request

2.4.1 The features that the second auxiliary request adds to the independent claims of the main request are technical features of the portable token service provider, expressed in the form of program features in an object-oriented language.

2.4.2 Independent claims 1 and 45 however contain broad and vague wordings which the board had to interpret in the light of the description for the purpose of the assessment of inventive step.
In that respect, the features of "attribute management services among a plurality of other token service provider interfaces" and "common services that can be used among differing control interfaces associated with the portable token service provider" are to be construed as representing, respectively, the services identified as "GetAttrib" and "SetAttrib" on pages 25-26 of the description, and the services identified as "GetCertificateList", "ChangePin", "DeactivatePin" and ""ReactivatePin" on pages 27-28 of the description. Moreover, the wording "services of an identified key pair" have been construed by the board as meaning the methods "Sign" and "Decrypt" as defined on pages 36-37 of the description.

2.4.3 As mentioned in paragraph 2.2.1 above, the portable token service provider defined in the claims can be read onto the ICC Resource Manager of D2. D2 discloses (see part 5) that the ICC Resource Manager makes services and cryptographic data within an ICC accessible to a cryptographic server provider using an exposed functional interface. It is considered to be implicit from D2 that these services and data encompass key pairs, certificate and cryptographic functions, and encryption and identification methods using the same, usually stored in and/or performed by an ICC. The cryptographic data and functions provided by the portable token service provider objects as defined by the additional features of independent claims 1 and 45 are therefore disclosed in D2.

Furthermore, the board agrees with the Examining Division's opinion, expressed in the minutes of the oral proceedings held in examination and in the decision to refuse, that creating different objects for the different functions of the portable token service provider and creating a hierarchy for them by grouping common features in parent objects are the basis of object-oriented programming. Since D2 clearly points out to an objet-oriented programming of the cryptographic system (see in particular part 5, point 3 and part 6, point 3) and since no surprising effect is achieved by such a programming, the board judges that the additional features of the second auxiliary request do not add anything of inventive significance to the subject-matter of the independent claims.

For these reasons, the independent claims of the second auxiliary request do not meet the requirement of Article 56 EPC 1973.

3. Therefore, neither of the three requests is allowable.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar The Chair

K. Götz A. Ritzka