Internal distribution code:

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

Datasheet for the decision of 11 December 2018

Case Number: T 1021/14 - 3.4.03

Application Number: 05702237.8

Publication Number: 1704541

IPC: G07F7/10, G07F19/00

Language of the proceedings: EN

Title of invention:
ELECTRONIC TRANSACTION SYSTEM AND A TRANSACTION TERMINAL ADAPTED FOR SUCH A SYSTEM

Applicant:
Gemalto SA

Headword:

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

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 1021/14 - 3.4.03

D E C I S I O N
of Technical Board of Appeal 3.4.03
of 11 December 2018

Appellant: (Applicant)	Gemalto SA 6, rue de la Verrerie 92190 Meudon (FR)
Representative:	Milharo, Emilien Gemalto SA Département Propriété Intellectuelle Avenue du Jujubier BP 90, Z.I. Athélia IV 13705 La Ciotat (FR)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 12 December 2013 refusing European patent application No. 05702237.8 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	C. Heath
Members:	M. Stenger
	S. Ward

Summary of Facts and Submissions

I. The appeal concerns the decision of the Examining Division to refuse European patent application No. 05702237 for non-compliance with the requirements of Article 123(2) EPC and for lack of inventive step.

II. The appellant requested that the contested decision be set aside and that a patent be granted according to the request consisting of claims 1 to 5 submitted with letter dated 9 November 2018, filed in reply to a preliminary opinion of the Board sent out in preparation of the oral proceedings.

III. Reference is made to the following document:

D1: US 2002/046185 A1

IV. Oral proceedings were conducted on 11 December 2018 in the absence of the appellant as indicated in the letter of reply to the preliminary opinion of the Board.

V. Claim 1 of the sole request has the following wording (labeling (a) to (d2) added by the Board):

A system for performing electronic transaction comprising:

(a) *a payment terminal including :*

(a1) *a human interface module (SPED) comprising a keyboard (KP), a display (D), a card reader (CR) for reading and authenticating a bank or credit card card, a processing means (MP) and an internal bus (B) for connecting these elements,*

(a2) *a hosting means (HT) connectable to the human interface module (SPED) through connection means (C1), said hosting means comprising a processing means and a memory (HTR), communication means, and a power supply (PS, EPS),*

(a3) *a first security module (ES),*

(b) *a gateway means (VTS) or a remote server of a service provider connectable to the hosting means (HT) through a telecommunication network (TN), said gateway means (VTS) being a virtual terminal server,*

(c1) *wherein a transaction terminal task manager is included in said first security module (ES),*
(c2) *said security module (ES) being hosted in said hosting means,*

(d) *wherein said human interface module (SPED)*
(d1) *executes transaction phases under said security module (ES) control,*
(d2) *and executes totally autonomously security treatments including presentation of the PIN code to the bank or credit card.*

VI. The arguments of the appellant (see grounds for appeal and letter dated 9 November 2018), insofar as they are

relevant to the present decision, may be summarised as follows.

(i) Shifting tasks from the transaction terminal to the security module led to a simplified structure of the human interface module.

(ii) Although the skilled person could have envisaged in a general manner to distribute tasks between different elements of a computer system, it was not obvious *how* to distribute these tasks in the *highly sensitive area of banking transactions*.

(iii) At the filing date of the application, the areas of banking and telecom were separated and it was inconceivable that a security module of a mobile phone controlled a banking terminal, for security and other reasons.

(iv) Although the SIM application toolkit allowed a SIM to perform certain tasks in a mobile phone, it did not suggest to control actions in an external device or disclose how that could be done.

(v) Nothing suggested a SIM that controlled only a part of the actions of the external device and explicitly not the PIN presentation to the card, whereby the system was rendered secure despite the transaction terminal task manager being included in the security module.

Reasons for the Decision

1. The appeal is admissible.

2. Article 123(2) EPC

The feature of a *security module for managing phases of said electronic transaction* objected to by the Examining Division (see second paragraph of page 3 of the contested decision) has been replaced in the current request by feature (d1) as defined above. Feature (d1) employs the terminology of the original description (page 2, lines 6 to 8 and page 4, lines 1 to 10 of the original description), as indicated by the appellant.

Thus, the Board is satisfied that amended feature (d1) overcomes the objection made by the Examining Division.

3. D1

D1 concerns the use of wireless communication devices like PDAs or mobile phones in conducting electronic POS transactions. The document mentions a plurality of different possibilities for distributing tasks between the individual modules of the computer system involved, these modules being, inter alia, the wireless communication devices, an EFTPOS terminal and a plurality of server systems.

4. Claim 1, D1

In the wording of claim 1, D1 discloses

A system for performing electronic transaction (see abstract) comprising:

(a) a payment terminal 302, 312 (see figure 3) including :

(a1) a human interface module 302 (paragraph 32, *handheld WAP appliance*) comprising a keyboard, a display, a card reader for reading and authenticating a bank or credit card card, a processing means and an internal bus for connecting these elements (this is implied by the context of the overall system of D1, see for example paragraph 30 and paragraph 32),

(a2) a hosting means 312 (paragraph 32, *second WAP device*) connectable to the human interface module 302 through connection means (paragraph 32, *via an RF or infrared signal*), said hosting means comprising a processing means and a memory, communication means, and a power supply (the second WAP device may be a mobile telephone, see paragraph 32, which implies the presence of these elements),

(a3) a first security module (a mobile/cellular telephone requires, in the standard GSM framework, the presence of a SIM card),

(c2) said security module (the SIM card) being hosted in said hosting means 312 (which may be a mobile/cellular phone, as mentioned before),

(b) a gateway means 316 (paragraph 32, *intermediate POS device*) or a remote server 226, 230 of a service provider (*consumer's service provider gateway*, *WAP server*) connectable to the hosting means 312 through a telecommunication network (see figure 3), said gateway means being a virtual terminal server (since it performs a part of the standard tasks of a POS terminal device).

5. Difference

It follows from the above that the subject-matter of claim 1 differs from D1 by the following features:

(c1) wherein a transaction terminal task manager is included in said first security module (ES),

(d) wherein said human interface module (SPED)
(d1) executes transaction phases under said security module (ES) control,
(d2) and executes totally autonomously security treatments including presentation of the PIN code to the bank or credit card.

6. Technical effects/objective technical problems to be solved

As mentioned above, D1 discloses a distributed computer system for conducting electronic POS transactions. In the context of such a system, the distinguishing features as defined above relate to two different issues as follows.

6.1 Features (c1) and (d)/(d1)

The Board notes that claim 1 does not specify *in which sense* the first security module is *secure*. Further, the Board is not aware of any particular technical effect achieved by using a *security* module, as opposed to *any* module, to control the execution of transaction phases.

Consequently, features (c1) and (d)/d1) do not have any technical effect related to security issues.

The Board notes that features (c1) and (d)/(d1) do not require more than that at least two unspecified transaction phases are performed under the security module's control.

In view of the above, the technical effect of these features is that the human interface module does not need to be as high-performing as if it had to control the execution of *all* transaction phases.

The objective technical problem to be solved may then be formulated as how to provide a human interface module with a simplified structure, as submitted by the appellant (see point VI.(i) above).

6.2 Feature (d)/(d2)

The autonomous presentation of the PIN code to a card by the human interface module implies the autonomous execution of other tasks of the PIN verification process by the human interface module as well, such as accepting an entered PIN and receiving and treating the reply of the card. These other tasks can equally be considered as security treatments in the sense of claim 1. Thus, feature (d)/(d2) comprises embodiments in which the autonomous steps executed by the human interface module do not go beyond the PIN presentation / verification process.

Other security treatments could be performed by any of the other modules of the distributed computer system.

D1 discloses an online PIN verification by a remote bank/data processing system DPS (see paragraphs 3 and 24).
As compared to that, feature (d)/(d2) has the technical effect that the PIN entered into the human interface module does not need to be transmitted to a different module.

The objective technical problem to be solved may in this case be formulated as how to provide an alternative secure PIN entry mechanism (see page 2, lines 3 to 5 of the description) in a distributed system.

7. Inventive step

Features (c1) and (d)/(d1) on the one hand and feature (d)/(d2) on the other hand achieve different technical effects and relate to different objective technical problems as argued above. Thus, for the purpose of assessing inventive step, these two feature groups do not need to be considered together, as argued by the appellant (see point VI.(v) above), but can be discussed separately.

7.1 Features (c1) and (d)/(d1)
Generally, the distribution of tasks between a plurality of elements of distributed computer systems (like main frames, terminals, personal computers, supercomputers, thin clients, thick clients) according to the performance of these elements and the possibilities of data exchange between them has always

been an issue in computer technology. In such systems, it is a normal aim for the skilled person to obtain a distribution that is optimally adapted for the respective situation. Further, in that context, any specific distribution of tasks usually involves only predictable advantages and disadvantages, respectively.

On a general level, this was not contested by the appellant. Concerning the argument of the appellant that nothing suggested *how* to distribute tasks in a distributed computer system in the *highly sensitive area of banking transactions* (see point VI.(ii) above), the Board notes that no specific adaptation to this sensitive area of banking transactions is apparent from the wording of claim 1; this applies particularly to the wording of the distinguishing features.

More specifically, D1 explicitly mentions a plurality of different specific distributions of tasks between various elements of such a distributed computer system (see, for example, the thin client solution presented in paragraph 22 to 24 as compared to the thick client solution described in paragraphs 25 to 27), with the overall aim of implementing POS transaction systems with low infrastructure costs (see paragraph 20). The skilled person reading D1 would thus consider changing the distribution of the tasks performed by the individual modules to optimise the system, e.g. to further reduce infrastructure costs.

Starting from D1 and being confronted with the objective technical problem of how to provide a human interface module/WAP appliance 302 with a simplified structure, the skilled person would thus readily consider shifting some of the tasks performed by the human interface module/WAP appliance 302 to *any*

suitable one of the other modules of the overall system disclosed in D1.

One of the modules disclosed in D1 is the second WAP appliance/mobile phone 312 which is provided, in the standard GSM framework, with a SIM card. It was generally known at the priority date of the application that such SIM cards could be used to initiate actions for use in various value-added services, i.e., to perform tasks going beyond standard telecommunication issues (as evidenced by the GSM 11.14 standard released in 2001 explicitly defines the *SIM Application Toolkit* (or STK).

Therefore, the skilled person would regard the SIM card implied by the mobile telephone 312 as *one of the suitable modules* he could choose from when trying to shift one or more tasks away from appliance 302.

The Board notes that using a SIM in this manner implies the provision of a corresponding *task manager* in the SIM in the sense of feature (c1).

Thus, the skilled person would in this manner, using his common general knowledge, incorporate features (c1) and (d)/(d1) into the system known from D1 without the exercise of an inventive step according to Article 56 EPC 1973.

7.2 Feature (d)/(d2)

As mentioned before, D1 discloses an online PIN verification by a bank/data processing system DPS (see paragraphs 3 and 24). However, D1 also suggests that sending of the PIN the DPS may not be necessary (paragraph 24, *personal identification numbers or messages that may need to be sent to DPS 140*).

Further, D1 discloses that the cards involved can be smart cards/chipcards (see paragraphs 22 and 23).
For this type of cards, offline PIN verification by the cards themselves was, at the priority date of the application, a commonly known alternative to online PIN verification, with generally known advantages and disadvantages. For such offline PIN verifications, class 2 or 3 smart card readers with integrated keypads were (and are still) commonly used, for example in the framework of HBCI banking. These readers are provided with an integrated keyboard and present in an autonomous manner the PIN entered by a user on the keyboard to the smart card inserted in the reader, which then verifies the entered PIN. Thereby, any transmission of the PIN over a bus system or a network is avoided which enhances the security of the system.

Thus, starting from D1 and being confronted with the problem of how to provide an alternative way to securely enter PINs, in particular for smart cards/ chipcards, the skilled person, using his common general knowledge, would readily implement an offline PIN verification system according to feature (d2) in the system of D1 without exercising an inventive step according to Article 56 EPC 1973.

Irrespective of these considerations, the Board notes that the choice of a particular one of generally known cardholder verification methods (CVMs, e.g. online PIN verification, offline PIN verification, signature comparison, ID card control or any combination of these methods) is an administrative decision of the financial institution issuing the card.
Such a decision will be based on a trade-off analysis taking into account the security of the methods against

certain attacks, the complexity and cost of the system required and the risk/amount of money involved. The issuing institution may even choose not to verify the identity of the cardholder at all.

7.3 Further arguments of the appellant

7.3.1 Point VI.(iii)
The system of D1 has the purpose of executing payment transactions (see, for example, claims 1 and 2) and it involves a cellular phone, as argued above (see for example paragraphs 29 and 32). Therefore, the Board cannot accept the argument of the appellant that the areas of banking and telecom were separated at the filing date of the application and that it was therefore inconceivable at that date that (a security module of) a mobile phone controlled a banking terminal.

7.3.2 Point VI.(iv)
The Board notes that the initiation of actions as foreseen by the STK in a distributed computer system has an impact on the other modules of the computer system as a whole at least in the sense that the execution of tasks in the other modules is triggered. This must be seen as *controlling the execution of transaction phases* in these other modules according to the very general formulation of feature (d1).

7.4 It follows from the above that the subject-matter of the independent claims is not inventive according to Article 56 EPC 1973 in view of D1 combined with the common general knowledge of the skilled person.

8. Additional remark

The arguments presented above are based on an interpretation of claim 1 that involves separate human interface and security modules SPED and HT, respectively. However, figure 2 and the corresponding part of the description (page 5, first paragraph) relate to an embodiment where these modules are grouped in one single device.
A standard transaction terminal as referred to on page 1, lines 17 to 20 of the description must have at least one module that performs functions related to PIN entry; this module can be considered to be a *security module* in the sense of the application.
Therefore, the Board is not aware of any difference between the embodiment according to which the modules are grouped in one single device and a standard transaction terminal.

9. Since the only request on file does not fulfill the requirements of the EPC, the appeal must fail.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

S. Sánchez Chiquero C. Heath

Decision electronically authenticated