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 October 2018

Case Number:	T 0876/14 - 3.5.06
Application Number:	01910964.4
Publication Number:	1277162
IPC:	G06F1/00, G06K5/00, H04L29/06
Language of the proceedings:	EN

Title of invention:
FIELD PROGRAMMABLE SMART CARD TERMINAL AND TOKEN DEVICE

Applicant:
OneSpan International GmbH

Headword:
Electronic token device/ONESPAN

Relevant legal provisions:
EPC 1973 Art. 84, 83
EPC Art. 123(2)

Keyword:
Claims - support in the description (no)
Sufficiency of disclosure - completeness of disclosure
Amendments - added subject-matter (yes)

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

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 0876/14 - 3.5.06

DECISION
# of Technical Board of Appeal 3.5.06
of 11 October 2018

Appellant:
(Applicant)

OneSpan International GmbH
World-Wide Business Center
Balz-Zimmermannstrasse 7
8152 Glattbrugg (CH)

Representative:

Beck, Michaël Andries T.
IPLodge bvba
Technologielaan 9
3001 Heverlee (BE)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted on 27 November 2013 refusing European patent application No. 01910964.4 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman S. Krischer
Members: A. Teale
A. Jimenez

Summary of Facts and Submissions

I. This is an appeal against the decision, dispatched with reasons on 27 November 2013, to refuse European patent application No. 01 910 964.4 on the basis that the amendments to the application did not comply with Article 123(2) EPC.

II. During examination proceedings the applicant (now appellant) filed the following documents as evidence of common general knowledge at the priority date:

D14: K.P. Weiss, "When A Password Is Not A Password", Proceedings IEEE 1990 International Carnahan Conference on Security Technology: Crime Countermeasures, pages 100 to 108, 10 to 12 October 1990.

D15: "DIGIPASS 500 User's Manual", Document Revision 1.2, March 1999, Vasco Data Security, Document Nr. 750576.

III. A notice of appeal and the appeal fee were received on 29 January 2014, the appellant requesting that the decision be set aside and a patent granted.

IV. With a statement of grounds of appeal, received on 4 April 2014, the appellant filed amended claims according to a main and first to fourth auxiliary requests. The appellant also made an auxiliary request for oral proceedings.

V. In an annex to a summons to oral proceedings the board set out its provisional opinion that *inter alia* the feature in claim 1 of the main request "and to derive a token device key, resulting from generating of said token device personality" and similar features in claim 1 of all the auxiliary requests seemed to lack support by the description, Article 84 EPC 1973, and to be added subject-matter, Article 123(2) EPC.

VI. At the oral proceedings, held on 11 October 2018, the appellant filed amended claims according to a new auxiliary request 5 and requested that the decision be set aside and that a patent be granted on the basis of the main request or one of the auxiliary requests 1 to 4 all filed with the grounds of appeal, dated 4 April 2014, or on the basis of auxiliary request 5 dated 10 October 2018 [sic], filed during oral proceedings. At the end of the oral proceedings the board announced its decision.

VII. The application is thus being considered in the following form:

Description (all requests): pages 2, 3, 8, 10 to 16, 18, 20 to 23, 28 and 29, as published, pages 1, 4 and 9 (pages 14,15,25 to 27 having been later withdrawn), received on 22 September 2008, pages 17 and 19, received on 7 November 2011, and pages 5 to 7 and 24 to 27, received on 21 November 2012.

Claims: 1 to 34 according to a main and first to fifth auxiliary requests, the main and first to fourth auxiliary requests having been received with the grounds of appeal and the fifth auxiliary request having been received in the oral proceedings of 11 October 2018.

Drawings (all requests): pages 1/9 to 6/9 (7/9 to 9/9 having been deleted), as published.

VIII. Claim 1 according to the main request reads as follows:

"An electronic token device for offering the functionality of a strong authentication token, the electronic token device comprising a handheld field programmable electronic smart card terminal (100) and a full sized ISO 7810 smart card (105); said smart card (105) having a smart card secret (154) and comprising a DES engine; the terminal (100) comprising: an externally accessible smart card reader (104) adapted to receive and communicate with said smart card (105); a RAM memory (144); and, a token personality logic; wherein said token personality logic is adapted to generate, with said smart card (105), a token device personality using said smart card secret by carrying out the following steps: sending a first value to said smart card as an input; receiving a second value from said smart card, said second value being derived from said first value and said smart card secret (154) by said DES engine; storing said second value in said RAM memory; and to derive a token device key, resulting from said generating of said token device personality."

IX. Claim 1 according to auxiliary requests 1 to 4 contains the feature of "using said second value as a secret in calculations to derive a token device key". Claim 1 according to auxiliary request 5 contains the feature of "using said second value as a secret in calculations for said offering of said functionality of a strong authentication token including at least one of challenge-response and signature paradigms".

Reasons for the Decision

1. The admissibility of the appeal

In view of the facts set out at points I, III and IV above, the appeal fulfills the admissibility requirements under the EPC and is consequently admissible.

2. Summary of the invention

2.1 The invention relates to electronic token devices used, for example, to generate time-based dynamic passwords, otherwise known as "one-time passwords" (OTPs), which the user enters into an application on a computer, for instance for the purposes of home banking: see page 3, lines 19 to 21, and page 21, lines 15 to 22.

2.2 In the past, such tokens were self-contained units; see, for example, D14 and D15, cited by the appellant. However the invention allows the same "strong authentication token" functionality to be realized by combining an existing personalised smart card (see figure 1; 105) with a generic terminal device (figure 1; 100). According to page 11, lines 19 to 21, the "innovative terminal device replaces the tokens that have to provide secure remote access to Internet, phone banking and other banking services". Moreover the secure applications of the token device are designed to be "compatible with legacy systems and legacy tokens", for instance handling the generation of time- or event-based dynamic passwords and the challenge/response paradigm, see page 21, lines 15 to 22.

2.3 The smart card is a "full size" card adhering to the ISO 7810 standard (see page 19, lines 11 to 14) and comprises a smart card secret (see figure 6; 154) and a DES (Data Encryption Standard) engine; see page 26, lines 8 to 11. The board understands ISO 7810 in this context to refer to the 1995 version of the standard specifying the physical characteristics, such as the dimensions, of smart cards. In view of figures 1 and 2, the board understands "full size" to mean the ID-1 format of 85.60 × 53.98 mm commonly used for credit cards. The appellant has not disputed this interpretation.

2.4 As shown in figure 6, and described on page 26, lines 3 to 15, the terminal device comprises a card reader (150), a RAM memory (144) and a processing unit (148) (termed the "token personality logic" in the claims). In use, the terminal device generates a "token device personality", meaning that, as explained by the appellant at the oral proceedings, the smart card generates a user-specific secret (the "new value", termed the "second value" in the claims) which is stored in the RAM of the generic terminal to "program" the terminal. In this sense, the terminal is "field programmable", as opposed to being "pre-programmed" before it is issued to the user; see page 8, lines 7 to 11. To do this, the processing unit sends a first value to the DES engine of the smart card which returns a new value derived from the first value and the card secret. The token device uses this secret in subsequent calculations, for instance to produce a so-called "token device key" (see page 26, lines 11 to 12, and claim 1 of the main and first to fourth auxiliary requests), or to realize at least one of the challenge-response and signature paradigms (set out in claim 1 of the third and fifth auxiliary requests).

3. Added subject-matter, Article 123(2) EPC, support by the description, Article 84 EPC 1973, and sufficiency of disclosure, Article 83 EPC 1973

3.1 The board points out that the question of added subject-matter depends on whether the application contains subject-matter extending beyond the content of the application **as filed**, whilst support and sufficiency depend on the application **as it now stands.** The distinction is significant in the present case, since the appellant has deleted figures 8, 9 and 10 (drawing sheets 7/9 to 9/9), relating to the "medium", "high" and "very high" security modes, respectively, and the corresponding passages in the description relating to the "medium" and "very high" security modes, on pages 25, 26 and 27. Hence the most detailed disclosure of the invention is now provided by the passage relating to the high security mode on page 26, lines 1 to 15.

3.2 According to the reasons for the appealed decision, the feature in claim 1 according to the requests then on file "using said second value as a secret in calculations to derive a token device key; and wherein said smart card terminal (100) further comprises a communications mechanism comprising a display (107) for communicating said token device key to a user for an application provided by a service provider, said token device key resulting from said generating of said token device personality" was not directly and unambiguously derivable from the application as originally filed, Article 123(2) EPC. The application did not explain what the calculations mentioned on page 26, line 12, were and how the result of the calculations was used. Page 26, lines 1 to 15, concerning the "high security mode" stated (see lines 11 to 12) that "From then on the token device will use this secret in the calculations." This did not necessarily mean the derivation of a token device key as claimed.

3.3 Claim 1 according to the present main and first to fourth auxiliary requests still refers to the token device key "resulting from said generating of said token device personality" or to "using said second value as a secret in calculations to derive a token device key".

3.4 In its provisional opinion the board expressed doubts as to whether the description supported these expressions, Article 84 EPC 1973.

3.5 According to the appellant, an implicit disclosure was enough, and the skilled reader would have interpreted the features of the high security mode embodiment (page 26, lines 1 to 15) without using figure 9 (now deleted) as supporting the claimed subject-matter. In view of D14, the terms "password" or "secret" did not restrict the type of calculations or imply the use of information as an input to a cryptographic algorithm. The appellant has argued that the claimed subject-matter, in particular that of the first auxiliary request, is based on the "high security mode" disclosed in the application; see present page 26, lines 1 to 15. The skilled person would also have interpreted the statement on page 26, lines 11 to 12, concerning the value calculated by the smart card "From then on the token device will use this secret in **the calculations**" (emphasis by the board) as referring to cryptographic token calculations of the terminal.

3.6 In the oral proceedings the board also raised the objection that the same facts also showed that the application did not disclose the invention in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art, Article 83 EPC 1973. The appellant argued that the "token device personality" was the same as the "second value". Moreover the skilled person seeking to make the combined terminal/smart card compatible with legacy systems and legacy tokens (see page 21, lines 15 to 16), so as to replace them (see page 11, lines 19 to 21), would have known how to derive a token device key, depending on the functionality to be emulated (such as the challenge/response or signature paradigms), resulting from generating said token device personality, in particular from the new/second value. The derivation was a matter of interfacing with the smart card, in particular dealing with the required input and output formats, and, being usual matters for the skilled person, did not need to be stated in the application.

3.7 The board is not persuaded by the appellant's arguments and finds that the feature in claim 1 of the main request "and to derive a token device key, resulting from generating of said token device personality" and similar features in claim 1 of the first to fourth auxiliary requests lacks support by the description. The only possible support for this expression is on page 26, lines 11 to 12, which states that "From then on the token device will use this secret in the calculations". However this passage does not disclose how the token device key is derived. Even if matters of interfacing were known to the skilled person, the claimed derivation of a token device key goes beyond mere interfacing/formatting and may include mathematical derivation steps, for example. The application does not give a single example of such a derivation.

3.8 Claim 1 according to the fifth auxiliary request no longer sets out the derivation of a token device key. Instead, it sets out the feature of "using said second value as a secret in calculations for said offering of said functionality of a strong authentication token including at least one of challenge-response and signature paradigms".

3.9 In the oral proceedings the board raised the objection that the application, for instance on page 26, lines 12 to 15, only disclosed the use of the new/second value to derive the token device key. There was no hint at combining this disclosure with that on page 21 relating to the various legacy token functions. In particular, the application did not disclose using said second value as a secret in calculations to provide the functionality of a strong authentication token including the challenge-response and signature paradigms, as now set out in claim 1.

3.10 The appellant argued that the calculations referred to on page 26, lines 11 to 12, applied to all legacy token functions, indeed all the legacy token functions were mathematically equivalent to the generation of an OTP, a key being a response to a challenge. Furthermore original claim 9 referred to at least one of the applications stored in the terminal supporting security paradigms, including challenge-response and signature.

3.11 The board does not accept the appellant's arguments because, even if a key is a response to a challenge, the appellant has not shown that using the second value as a secret in calculations to provide the functionality of a strong authentication token including the challenge-response and signature paradigms is directly and unambiguously derivable from the application as originally filed (Article 123(2) EPC), in particular original claim 9, which does not mention the new/second value. The appellant has also provided no evidence that all the legacy token functions are mathematically equivalent to the generation of an OTP.

4. Conclusion

4.1 The board finds that the application according to the main and first to fourth auxiliary requests does not comply with Articles 84 and 83 EPC 1973 regarding support by the description and sufficiency of disclosure, and the application according to the fifth auxiliary request does not comply with Article 123(2) EPC regarding added subject-matter.

4.2 Hence none of the appellant's requests complies with the EPC.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

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

I. Aperribay S. Krischer

Decision electronically authenticated