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 August 2017

Case Number: T 2304/14 - 3.5.03

Application Number: 11171212.1

Publication Number: 2538641

IPC: H04M1/725, H04L29/08

Language of the proceedings: EN

Title of invention:
Secure tag management method and system

Applicant:
Swisscom AG

Headword:
Secure tag/SWISSCOM

Relevant legal provisions:
EPC Art. 56, 84

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

Europäisches Patentamt
European Patent Office
Office européen des brevets

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 2304/14 - 3.5.03

D E C I S I O N
of Technical Board of Appeal 3.5.03
of 3 August 2017

Appellant: (Applicant)	Swisscom AG Alte Tiefenaustrasse 6 Worblaufen / Ittigen 3050 Bern (CH)
Representative:	BOVARD AG Patent- und Markenanwälte Optingenstrasse 16 3013 Bern (CH)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 4 July 2014 refusing European patent application No. 11171212.1 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	F. van der Voort
Members:	B. Noll
	P. Guntz

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division refusing European patent application No. 11171212.1 (publication No. EP 2 538 641 A1) on the ground that the claimed subject-matter according to a main request and three auxiliary requests lacked novelty (Article 54 EPC).

II. With the statement of grounds of appeal, the appellant filed sets of claims of a main request and an auxiliary request.

III. In a communication accompanying a summons to oral proceedings, the board gave its preliminary opinion that the subject-matter of claims 1 of each request did not involve an inventive step.

The following documents were referred to in the communication:

D2: US 2006/0094411 A1; and

D3: J. Carstens: "GOX Fuse ROM fuer RFID-Chips", IP.com Technical Disclosure, 1 March 2006, page 1.

IV. With a letter dated 27 July 2017, the appellant filed claims of an amended main request, an amended first auxiliary request, and a new second auxiliary request together with arguments in support of inventive step.

V. Oral proceedings before the board were held on 3 August 2017.

In the course of the oral proceedings, the appellant filed a set of claims of a third auxiliary request.

The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the claims of the main request or, in the alternative, on the basis of the claims of either the first or the second auxiliary request, these requests as filed with the letter dated 27 July 2017, or on the basis of the claims of the third auxiliary request as filed during the oral proceedings.

At the end of the oral proceedings, the chairman announced the board's decision.

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

"A system comprising a mobile communications device (1) running an application (2), a contactlessly readable tag (4), and a tag management server (7), the system being configured for controlling a function of the mobile communications device (1) by means of the application (2) in dependence upon data read from the tag (4),

the tag (4) comprising a storing means for storing tag-identifying data (5), the tag-identifiying *[sic]* data (5) being stored in the storing means of the tag (4) in a unalterable way,

the mobile communications device (1) comprising a tag identifying means for contactlessly reading tag identifying data (5) from the tag (4), and a data request transmission means for sending a data request signal (19a, 25) with the tag identifying data (5) to the tag management server (7),

the tag management server (7) comprising a database (8) comprising one or more data records (15, 16, 17, 18), each data record (15, 16, 17, 18) containing instructions and/or parameters for controlling a function,

characterized in that

the tag management server (7) is capable of receiving the tag identifying data (5) and parameters stored in the application (2) of the mobile communication device (1) from the mobile communication device (1), and that

the tag management server (7) selects record data (15) stored in the database (8), said database (8) being a controlled database (8) which can be continuously monitored, tested and defended against malicious attacks, based on the received tag identifying data (5) and parameters stored in the application (2) of the mobile communication device (1), and transmits said selected recorded data (15) to the application (2) for controlling the function of the mobile communications device (1),

whereby the application (2) of the mobile communications device (1) is adapted to receive the selected data record (15) and to execute the said instructions, and/or to process the said parameters of the selected data record (15), thereby performing the said function of the mobile communication device (1) in dependence on the instructions, and/or the parameters of the data record (15) selected in dependence upon the tag identifying data (5)."

Claim 1 of the **first auxiliary request** reads as follows:

"A system comprising a mobile communication device (1) running an application (2), a contactlessly readable tag (4), and a tag management server (7), the system being configured for controlling a function of the mobile communications device (1) by means of the application (2) in dependence upon data read from the tag (4),

the tag (4) comprising a storing means for storing tag-identifying data (5), the tag-identifiying *[sic]* data (5) being stored in the storing means of the tag (4) in a unalterable way,

the mobile communications device (1) comprising a tag identifying means for contactlessly reading tag identifying data (5) from the tag (4), and a data request transmission means for sending a data request signal (19a, 25) with the tag identifying data (5) to the tag management server (7), wherein

the tag management server (7) is capable of receiving the tag identifying data (5) from the mobile communication device (1), identifying the instructions and/or parameters associated with the received tag identifying data (5) and for transmitting said instructions and/or parameters to the application (2) for controlling the function of the mobile communications device (1),

characterised in that

an access address of the tag management server (7) is stored in the mobile communications device (1), the

tag (4) containing no data which can be used to access said tag management server (7), such data being only available to the application (2)."

Claim 1 of the **second auxiliary request** reads as follows:

"A system comprising a mobile communication device (1) running an application (2), a contactlessly readable tag (4) issued by a tag owner (6), and a tag management server (7), the system being configured for controlling a function of the mobile communications device (1) by means of the application (2) in dependence upon data read from the tag (4),

the tag (4) comprising a storing means for storing tag-identifying data (5), the tag-identifiying *[sic]* data (5) being stored in the storing means of the tag (4) in a unalterable way,

the mobile communications device (1) comprising a tag identifying means for contactlessly reading tag identifying data (5) from the tag (4), and a data request transmission means for sending a data request signal (19a, 25) with the tag identifying data (5) to the tag management server (7),

characterized in that

the tag (4) containing *[sic]* neither data which can be used to access to said tag management server (7), such data being only available to the application (2), nor any function data, and that

the tag management server (7) comprises a database (8) storing one or more data records (15, 16, 17, 18)

under control of said tag owner (6), each data record (15, 16, 17, 18) comprising one or more instructions and/or parameter data (15') for controlling a desired function of the communication device (1),

wherein

the tag management server (7) is capable of receiving the tag identifying data (5) from the mobile communication device (1), and is arranged to select record data (15) comprising appropriate functional instructions and/or parameter data (15') depending on at least the received tag identifying data (5), and to transmit said functional instructions and/or parameter data (15') to the application (2) for controlling said desired function of the mobile communications device (1),

whereby the application (2) of the mobile communications device (1) is adapted to receive the selected data record (15) returned by the tag management server (7) and to execute the said appropriate functional instructions, and/or to process the said parameter data of the selected data record (15), thereby performing said desired function of the mobile communications device (1) in dependence on the functional instructions, and/or the parameter data (15') of the selected data record (15)."

Claim 1 of the **third auxiliary request** differs from claim 1 of the main request in that in the first paragraph the wording "a function" has been replaced by "a plurality of functions", in that in the fourth paragraph "a function" had been replaced by "a desired function", and in that in the last paragraph "the said

function" has been replaced by "the said desired function".

Reasons for the Decision

1. *The application*

The application in suit is concerned with the management of tag-based services for a user of a mobile communication device. A tag contains a transponder circuit and a small memory with data and can be scanned by a mobile communication device via a suitable interface for reading the data. The data read from the tag is processed in the mobile communication device for providing a tag-based service. So far, this is prior art as discussed in the application. In this prior art, the data read from the tag may contain a link to a website or code relating to instructions to be executed by the mobile communication device. It is further discussed that tag data is vulnerable if it can be manipulated, and the communication device of the user is then at risk of infection with malicious software.

The application in suit addresses this problem by proposing a system in which the tag does not store executable code. The tag only stores "tag-identifying data" to be used by the mobile communication device for accessing further information on a tag management server. Any executable code for controlling a function of the mobile communication device relating to the selected tag service is present only in the tag management server. If requested, this information is transmitted from the server to the mobile communication device. The data stored in the tag itself does not therefore exercise any control over the mobile communication device.

2. *Claim 1 of the main request - inventive step (Article 56 EPC)*

2.1 The system of claim 1 of the main request lacks inventive step (Articles 52(1) and 56 EPC) for the reasons set out below.

2.2 Document D2 discloses a system which is configured to control a function of a mobile station (101 in Fig. 1 or 200 in Fig. 2) by means of an application 209 executed on the mobile device and dependent upon data read from an RFID tag 221. The overall system is shown in the block diagram in Fig. 1. Various embodiments relating to specific scenarios for providing services on the basis of the tag data read by the mobile communication device from the RFID tag are shown in Figs. 3, 4, 6 and 7. In particular:

(a) Fig. 3 shows an embodiment relating to a tag-based call forwarding service;

(b) Fig. 4 shows an embodiment relating to the automatic payment of a parking fee;

(c) Fig. 6 shows an embodiment in which selectable services are offered in response to processing tag data; and

(d) Fig. 7 shows an embodiment for use at a bus stop, in which a bus driver may be notified that a user is waiting and in which the user may download a bus timetable.

The system disclosed in D2 includes an RFID tag 127 for storing data and for being contactlessly read by the

mobile station (200, Fig. 2) over an air interface 125, 223 (paragraphs [0028] and [0033]). The data stored in the tag is for accessing e.g. application server 609 (cf. paragraph [0051]) in order to provide to the user a service associated with the tag. The data for accessing the transaction server stored on the tag is therefore "tag-identifying data" within the wording of claim 1.

The mobile station 200 is a mobile communication device within the wording of claim 1. It comprises an RFID interrogator (219, cf. Fig. 2) as a tag-identifying means for having a radio communication with the tag and reading tag-identifying data from the tag (cf. paragraph [0051], second sentence). A connection is established between the mobile station and an application server (e.g. 609 in Fig. 6) based on the data read from the tag (see paragraph [0051], "*The mobile station 601 may then use the RFID tag information to access, through a service provider of mobile station 601, the RFID application server 609 using any suitable protocol and any suitable wireless interface of which mobile station 601 is capable*"). This implies that the mobile station has a data request transmission means and that it sends a data request signal with the tag-identifying data to the application server.

The application server may download an applet to the mobile station, the applet causing the mobile station to display a service selections menu to the user for subsequently downloading further applets in response to a selection of a service by the user (paragraph [0052]). The application server is therefore a tag management server and the applets are data records of a database containing instructions for controlling one or

more desired functions of the mobile communication device. The application server is thus capable of receiving the tag-identifying data and parameters stored in the application of the mobile station. Parameters are implicitly the address information of the mobile station in the network, as the application server needs to know to which device the applet is to be sent. On the basis of the received request and the parameters, the application server selects a data record, i.e. an applet matching the request corresponding to the tag information, and transmits the selected data record, i.e. the applet, to the application. It is implicit that the operating system 207 (Fig. 2) and those of the applications 209 that are responsible for controlling the execution of an applet at the mobile station are an "application" within the wording of claim 1, for controlling the function of the mobile station. Hence, the operation system and the applications responsible for executing an applet at the mobile station are adapted to receive and execute the applet, thereby performing the function of the mobile station depending on the instructions and parameters contained in the applet. In the example described in D2 in paragraph [0052], functions performed include e.g. displaying by the mobile station a service selection menu for the user, accepting service selections from the user or initiating a download of further applets.

As regards the feature in claim 1 that the database is a controlled database "which can be continuously monitored, tested and defended against malicious attacks", the board is of the view that this feature does not limit the claimed system, since any server, including the application server 609 in D2, can be configured in this way in order to protect its database. This feature therefore does not further

distinguish the claimed system from the disclosure of D2.

2.3 The appellant argued that the system disclosed in D2 did not provide a selection of a data record based on tag-identifying data. The URL stored in the tag as mentioned in paragraph [0045] of D2 could not be considered as tag-identifying data, since it served the sole purpose of routing information through a communication network to a server. The URL was not suitable to select data at the server.

2.4 The board does not agree. The skilled person would appreciate that the URL mentioned in D2 identifies the service the mobile station is able to access as well as the information relating to the selected service. The URL serves to select the desired data record at the server for subsequent transmission to the mobile station and is, therefore, "tag-identifying data" within the wording of claim 1. The fact that the URL also serves for routing information through the network is not relevant in this respect.

2.5 In view of the above, the system as claimed thus differs from the disclosure of D2 in that the tag-identifying data is stored in the storing means of the tag in an unalterable way.

Storing tag-identifying data in an unalterable way renders the data stored in the tag immune to any modification. Therefore, the tag itself is made tamper-proof. The underlying technical problem solved may therefore be seen in protecting the tag content against unauthorised manipulation.

The skilled person faced with this technical problem would have considered document D3, as it discloses that an RFID circuit memory may be configured such that it can be programmed only once (cf. page 1, first and seventh paragraphs "...die nur eine einmalige ... [Programmierung] erlauben und sonst nur zum Lesen verwendet werden koennen" and "Nach Programmierung aller Bloecke, d.h. wenn alle Zeiger-bits gebrannt sind, erlaubt der Chip lediglich noch die Lesefunktion"), thereby inherently protecting the content of the RFID circuit against unauthorised amendment. The skilled person, starting out from D2 and aiming at making the tag tamper-proof, would thus be led by the teaching of D3 to store information in the memory of the tag in an unalterable way and, in doing so, would thereby arrive, without the exercise of inventive skill, at a system which includes all the features of claim 1.

2.6 The appellant argued that all data stored in the memory of an RFID tag in D3 was securely stored. In the present application, however, it was foreseen that only the tag-identifying data was stored in an unalterable way.

The board is not convinced by this argument. The wording of claim 1 does not specify how other data is stored in the memory of the tag. Therefore, claim 1 does not require that the tag-identifying data is stored in an unalterable way, whereas other data is not.

2.7 The subject-matter of claim 1 of the main request therefore lacks inventive step (Articles 52(1) and 56 EPC). The main request is therefore not allowable.

3. *Claim 1 of the first auxiliary request - inventive step (Article 56 EPC)*

3.1 In the call-forwarding service embodiment in D2 as shown Fig. 3, the system comprises a mobile communication device (mobile station 301), a contactlessly readable tag (RFID tag 305) and a tag management server (MSC 113, Fig. 3) and is configured for controlling a call forwarding operation of the mobile station (cf. paragraph [0037]). The tag comprises a storing means for storing a wireline telephone number of a wireline telephone 303. The wireline telephone number is tag-identifying data within the wording of claim 1. The mobile station comprises a tag-identifying means for contactlessly reading the tag-identifying data from the tag (cf. paragraph [0035]). In the embodiment of Fig. 3, call forwarding requested by the mobile station includes a forwarding operation with MSC 113 such that any calls to the mobile station are forwarded to the wireline telephone 303 (paragraph [0037]). This request is a data request in the wording of claim 1. The mobile station therefore comprises a data request transmission means of sending a data request signal with the tag-identifying data to the tag management means. The MSC is capable of receiving the wireline telephone number read by the mobile station from the RFID tag, and setting up the automatic forwarding of calls to this telephone. The communication between the mobile station and the MSC for setting up the call forwarding implicitly includes a transmission of instructions or parameters from the MSC to the mobile station.

3.2 Accordingly, the system of claim 1 differs from the system shown in Fig. 3 of D2 in that the tag-identifying data is stored in the storing means of the

tag in an unalterable way, and that an access address of the tag management server is stored in the mobile communications device, the tag containing no data which can be used to access the tag management server, such data being only available to the application.

Storing tag-identifying data in an unalterable way leads, as stated above, to a tag which is more resistant to unauthorised modification of its data content. Storing an access address of a tag management server in the mobile communication device has the effect that the mobile communication device is capable of contacting the tag management server, independent of information received from the tag.

Therefore, starting out from the Fig. 3 embodiment of D2, the technical problem to be solved by the skilled person can be formulated as to conveniently and robustly implement a call-forwarding service using an RFID tag.

3.3 The skilled person starting out from D2 and faced with this problem would appreciate that the "RFID push-to-call" service described in paragraph [0059] of D2 uses the telephone number stored in the tag itself and would consider storing this number in the tag in an unalterable way, as disclosed in D3, for the same reasons as set out at point 2 above. Since call forwarding is provided by the service provider to the user of the mobile station, the skilled person would consider setting up the system such that the request for call forwarding is sent to the service provider of the mobile communication device. Further, the skilled person would not consider storing this access data in the tag itself, since the identity and, hence, the address, of the service provider is determined by the

user's service contract for the mobile station which interrogates the RFID for the purpose of reading out the telephone number to which calls are to be forwarded. The skilled person would therefore consider using the address data of the service provider stored in the mobile station as the recipient of the request for call forwarding. Therefore, the skilled person would use, without the exercise of inventive skill, the information relating to the address to which a request for call forwarding is to be sent in the requesting mobile station itself, i.e. not in the tag, and would thereby arrive at the claimed system without the exercise of inventive skill.

3.4 The appellant argued that it was conceivable that the call forwarding request in D2 was first sent to an application server which then continued with further setting up the call forwarding process with the MSC. Hence, it was not implicit in D2 that the address of the tag management server was stored in the application in the mobile communication device.

3.5 This argument is not convincing. The skilled person may further consider an implementation as explained by the appellant. However, this does not mean that the skilled person would not consider sending the request directly from the mobile station to the MSC as explained above.

3.6 The subject-matter of claim 1 of the first auxiliary request therefore does not involve an inventive step (Articles 52(1) and 56 EPC). The first auxiliary request is therefore not allowable.

4. *Claim 1 of the second auxiliary request - clarity (Article 84 EPC)*

4.1 Claim 1 of the second auxiliary request is not clear (Article 84 EPC).

4.2 In particular:

(a) It is not clear which technical limitation is implied by the feature that the tag is "issued by a tag owner", see claim 1, first paragraph. The appellant argued that the tag owner was a technical component of the system as shown by block 6 in Fig. 3.

However, in the board's understanding, Fig. 3 explains steps for setting up and operating a tag service. The blocks in Fig. 3 do not necessarily represent technical components of the system. In fact, in examples 1 and 3 (paragraphs [0049] to [0051] and [0053] of the application as published) it is stated that the tag owner is respectively a circus company and a worker. A company or a worker is clearly not a technical component of a system.

(b) The meaning of the feature "function data" in the fifth paragraph of claim 1 is not clear.

The appellant referred to page 12, lines 31 to 33, and page 15, lines 2 and 3, and argued that "function data" comprised all instruction or parameter data which affected the function executed at the mobile communication device. Function data was therefore to be distinguished from tag-identifying data.

The board is however of the view that in the present case no distinction can be drawn between data based on whether or not it affects the operation of the mobile station, since the tag-identifying data itself has the function of downloading instructions from the tag

management server to the mobile communication terminal. Tag-identifying data too is therefore "function data" in this sense.

(c) It is further not clear which technical limitation is implied by the feature "under control of said tag owner", see claim 1, sixth paragraph. The appellant argued that it was solely the tag owner who could exercise control of the database or store data records therein. This is, however, not expressed by this wording, since it does not exclude the possibility that somebody other than the tag owner or another entity, e.g. the system administrator of the tag management server, may exercise control as well.

4.3 Claim 1 of the second auxiliary request is therefore not clear (Article 84 EPC). The second auxiliary request is therefore not allowable.

5. *Claim 1 of the third auxiliary request - inventive step (Article 56 EPC)*

5.1 The additional features included in claim 1 do not contribute to an inventive step.

5.2 The appellant argued that the application in D2 was not able to execute a plurality of functions, but only a single function.

5.3 The board does not agree. The skilled person would understand that the application in D2 serving to display a service selection menu to the user for selecting a desired service (see point 2.2 above) is configured for controlling a plurality of "functions", i.e. displaying the selection menu on the screen, detecting a user input and causing the downloading of

an applet relating to the selected service and controlling its execution. Therefore, the additional features in claim 1 do not further distinguish the claimed system from the disclosure of D2.

5.4 In view of the above and for the reasons set out in point 2 in respect of claim 1 of the main request, the subject-matter of claim 1 of the third auxiliary request does not involve an inventive step (Articles 52(1) and 56 EPC).The third auxiliary request is therefore not allowable.

6. Since none of the requests is allowable, it follows that the appeal is to be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

G. Rauh F. van der Voort

Decision electronically authenticated