Internal distribution code:

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

Datasheet for the decision of 9 December 2022

Case Number: T 0793/18 - 3.5.01

Application Number: 14741712.5

Publication Number: 3014545

IPC: G06Q20/42, G06F21/43

Language of the proceedings: EN

Title of invention:
TWO FACTOR AUTHENTICATION

Applicant:
Advanced New Technologies Co., Ltd.

Headword:
Two factor authentication/ADVANCED NEW TECHNOLOGIES

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - use of alphanumeric instead of QR verification code (no - obvious alternative)

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 0793/18 - 3.5.01

D E C I S I O N
of Technical Board of Appeal 3.5.01
of 9 December 2022

Appellant: (Applicant)	Advanced New Technologies Co., Ltd. Cayman Corporate Centre 27 Hospital Road George Town, Grand Cayman KY1-9008 (KY)
Representative:	McKinnon, Alistair James WP Thompson 138 Fetter Lane London EC4A 1BT (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 7 November 2017 refusing European patent application No. 14741712.5 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Chandler
Members:	M. Höhn
	Y. Podbielski

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division refusing European patent application No. 14741712.5 pursuant to Article 97(2) EPC on the grounds of lack of novelty (Article 54(1) and (2) EPC) over D3 (US 2010/131409 A1) and extension of subject-matter (Article 123(2) EPC).

In a section entitled "Further comments", objections for lack of inventive step (Article 56 EPC) were given over D1 (WO 2012/005653 A1) and D2 (GB 2 481 663 A).

II. In the statement setting out the grounds of appeal, the appellant requested that the appealed decision be set aside and that a patent be granted on the basis of the main request or first to third auxiliary request, all submitted with the statement setting out the grounds of appeal. Oral proceedings were requested if any request was unallowable.

III. In its annex to the summons to oral proceedings, the Board expressed its preliminary opinion that the requests lacked inventive step (Article 56 EPC) or were not allowable under Articles 84 and 123(2) EPC.

IV. In a reply dated 23 September 2022, the appellant submitted a sole request to replace the requests on file together with arguments in favour of inventive step.

V. By letter dated 17 October 2022 the Board was informed that the appellant would not be attending the oral proceedings and requested a decision according to the

state of the file. Oral proceedings to be held on 18 October 2022 were therefore cancelled.

VI. Independent claim 1 according to the sole request reads as follows:

"1. A method for authenticating user identity, comprising:

generating (210) a first verification code by a server (520), the first verification code including a first plurality of alphanumeric characters;

displaying (220), via a client terminal (510), the first verification code to a user in an application scenario of a service requiring user identity authentication, wherein the service is executed on the server, and wherein the first verification code is stored along with a user ID associated with the user;

displaying (225), via the client terminal (510), a prompt, comprising:

displaying, via the client terminal (510), the prompt in the application scenario, the prompt instructing the user to send a second verification code to the server (520) via an uplink message using an application other than the application scenario, the second verification code including a second plurality of alphanumeric characters;

receiving (230) the second verification code sent by the user via the uplink message using the application other than the application scenario;

comparing (240) the second verification code sent by the user and the first verification code generated by the server (520); and

determining (250) whether the user has passed identity authentication based on a result of the comparison, comprising:

in the event that the first plurality of alphanumeric characters of the first verification code matches the second plurality of alphanumeric characters of the second verification code:

retrieving, based on the first verification code, the user ID associated with the user;

comparing a user ID of the application other than the application scenario with the user ID associated with the user; and

in the event that the user ID of the application other than the application scenario matches the user ID associated with the user, determining (250) that the user has passed identity authentication and setting an uplink verification passed status on the server."

VII. The appellant argued essentially as follows:

After notification of the verification code via the application scenario, the server performs identity authentication based on the uplink message method defined in claim 1, and during identity authentication, the server ensures consistency of dynamic verification codes and the uplink mobile phone number with their preset values. In other words, security risks are not created due to leakage or Trojan horse interception of downlink message content.

None of the prior art publications on file taken alone discloses the combination of the features of claim 1. In particular, none of the publications teaches or discloses comparing a user ID of the application other than the application scenario with the user ID associated with the user.

A technical effect of the distinguishing features is to provide a more secure means of authenticating the identity of the user. In particular, after determining that the first plurality of alphanumeric characters of the first verification code matches the second plurality of alphanumeric characters of the second verification code, the system requires a further authentication step to authenticate the user. A user ID sent from the application responsible for sending the second verification code is further compared against the user ID registered on the server in order to satisfy the user identity check. This further step increases security in that the user identity authentication process is not satisfied until it receives double confirmation that the user has indeed sent the second verification code using the same application that sent the second verification code.

The objective technical problem may be formulated as how to provide a more secure means of authenticating the identity of the user. Taking D1 to be the closest prior art, and looking to solve the objective technical problem, the skilled person would have no motivation or hints to modify D1 in a manner that would arrive at something falling within the scope of the claimed subject-matter.

Whilst D1 also requires the user to actively partake in the user authentication process, the steps that the system requires the user to undertake are distinctly different to those defined by claim 1. The Board alleges that the session ID disclosed in D1 has the same function as the verification code according to the present invention. However, the session ID disclosed in D1 does not perform a further check after determining that the verification codes match. There is no teaching

of a further user ID check to confirm that a user has used the application to send a second verification code to the server as defined in claim 1.

Reasons for the Decision

1. The invention

The invention starts out from a conventional identity authentication method where a user accessing a system ("application scenario", e.g. for online payment) receives from a server an SMS text message on their mobile phone containing a randomly generated verification code (see [0005] of the originally filed application). The user enters this verification code into a login screen of the system and it is sent to the server. The server compares the received verification code against the previously sent verification code. If the two codes match, then the user is authenticated.

The invention addresses the security risk in this authentication method that hackers could possibly intercept these text messages and steal the victims' identity or funds (see [0007]).

The key idea of the invention is that the user enters the verification code (uplink) "*using an application other than the application scenario*". In the claim, the verification code and the prompt to enter the code are both displayed to the user in the application scenario (downlink).

An "application scenario" might be a web page for online payment, but can be any scenario requiring

identity authentication (see [0022]) and therefore is interpreted broadly. The other application could be an SMS message service (see [0033]) or a messaging application such as WeChat or QQ (see [0037]).

2. Article 56 EPC - Inventive step

The Board judges, in accordance with the "Further comments" in the decision under appeal, that the subject-matter of independent claim 1 lacks an inventive step.

2.1 The Board agrees with the appellant's understanding that D1 relates to a system for secure identification of a user (see letter dated 23 September 2022, page 3, paragraph 4). The system of D1 relies on the use of a QR code for authentication. As explained in D1 on page 12, line 34, the QR code is generated by the server side 50 and shown on the local device (i.e. client side terminal 20 in Figure 1) in the same application as the application scenario. The user 2 then uses their mobile telephone 10 to scan the QR code and send it to the server 50.

2.2 In view of this disclosure, the Board considers that the features outlined in point 17.1 of the decision were known from D1 when starting from this publication as closest prior art.

Hence, D1 discloses that the server side is configured to initiate a communication session with a local device over a data network, the communication session having a session ID, to generate a representation of the session ID and to transmit the representation to the local device over said data network. The local device is configured to present the representation in a user

interface of said local device. The mobile terminal is configured to capture the presented representation so as to derive said session ID, and to send a message containing the derived session ID to the server side over said data network (see Abstract and Figure 2).

2.3 In particular and in contrast to the appellant's arguments submitted with the statement setting out the grounds of appeal, D1 discloses the use of a different device than the terminal 20 on which the code is prompted (downlink 209 in figure 2), for submitting the code to the server (uplink 217 in figure 2), namely a mobile terminal 10. Even though it is called "the secure identification application" this application running on the mobile terminal is separate from the communication session to be authenticated on the terminal 20 and it is using a different communication link. It cannot therefore be considered part of "the application scenario" specified in claim 1 when interpreted broadly as mentioned in point 1 above, in contrast to the appellant's argumentation (see point 6.4 of the statement setting out the grounds of appeal), but is a different application.

The session ID disclosed in D1 has the same function as the verification code in the present invention (see above) and therefore anticipates this feature of claim 1. The PIN code referred to in D1 is an additional security measure for unlocking the mobile terminal 10, but has nothing to do with the authentication of the communication session.

2.4 In contrast to the appellant's argument that none of the publications teaches or discloses comparing a user ID of the application other than the application scenario with the user ID associated with the user, the

Board judges that this is known from D1 (see Abstract; page 10, lines 10 to 31; page 13, lines 3 to 11).

"The server side (50) is configured to initiate a communication session (42) with the local device (20) over the data network (40), said communication session having a session ID, to generate a representation (24) of the session ID and to transmit the representation to the local device over said data network. The local device (20) is configured to present the representation in a user interface (22) of the local device. The mobile terminal (10) is configured to capture the presented representation so as to derive the session ID, and to send a message containing the derived session ID to the server side over the data network. The server side is **further configured to determine an identity of the mobile terminal** on the telecommunications network, to **verify the determined mobile terminal identity against prestored reference data (56) which links the mobile terminal identity to private user information (54) pertaining to the user (2)**, and, upon successful verification, to associate the communication session with the private user information." (see Abstract of D1, emphasis added).

Therefore D1 does explicitly disclose after determining that the first verification code matches the second verification code, a further authentication step to authenticate the user. A user ID sent from the application responsible for sending the second verification code is further compared against the user ID registered on the server in order to satisfy the user identify check according to claim 1.

2.5 Hence the only distinguishing feature is, as expressed in the "Further comments" in the decision (see point

17.2), that the verification codes include alphanumeric characters instead of being QR codes.

2.6 Contrary to the appellant's arguments submitted with the statement setting out the grounds of appeal (see point 6.12), the Board doubts that the use of alphanumeric characters provides less chance of corruption than a QR-Code. But even so, the Board is of the opinion, as stated in the "Further comments" at point 17.3 of the decision, that it was obvious to use alphanumeric characters instead of QR Codes, because this was commonly known and practised in the art. This is also apparent from the conventional identity authentication method mentioned in the description of the present application (see [0005]) where text messages are used for transmission of verification codes. Hence, the use of alphanumeric characters does not involve an inventive activity.

2.7 The appellant's arguments to the contrary provided in writing do not convince for the aforementioned reasons.

2.8 Thus, the subject-matter of claim 1 of the sole request does not involve an inventive step over the disclosure of D1 combined with common general knowledge (Article 56 EPC).

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek W. Chandler

Decision electronically authenticated