Birch Stewart Kolasch Birch LLP

Protecting the Product of your Mind®

COSMOKEY SOLUTIONS VS. DUO SECURITY No. 2020-2043 (Fed. Cir. 2021). Link

Before O'MALLEY, REYNA, and STOLL, *Circuit Judges*

By: Alexander Taousakis

January 26, 2022

DISCUSSION

- CosmoKey Solutions GmbH & Co. KG appeals the United States District Court for the District of Delaware's entry of judgment on the pleadings holding that the asserted claims of CosmoKey's U.S. Patent No. 9,246,903 (herein the '903 patent) are ineligible under 35 U.S.C. § 101.
- The district court held that the asserted claims are directed to abstract ideas and fail to provide an inventive concept.

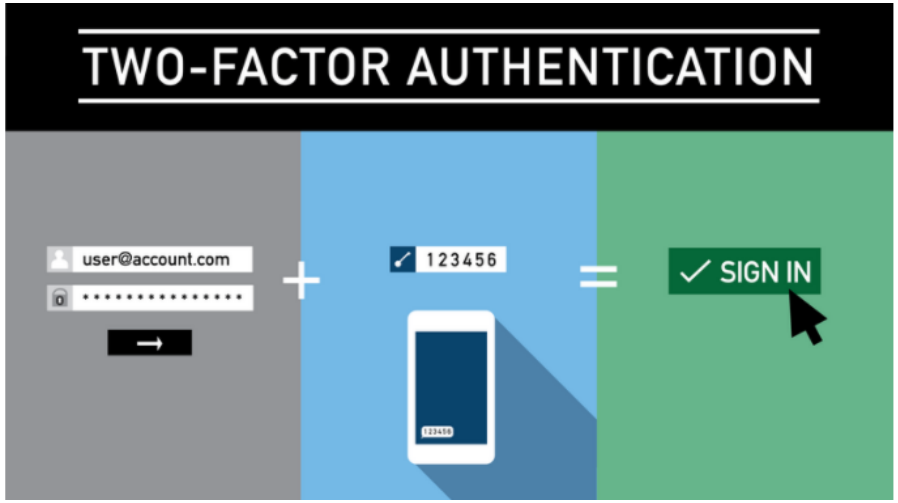
BACKGROUND

- The ’903 patent is titled “Authentication Method” and purports to disclose an authentication method that is both low in complexity and high in security. Patent Link.
- The abstract describes a method of authenticating the identity of a user performing a transaction at a terminal (e.g., a computer), including activating an authentication function on the user’s mobile device. ’903 patent Abstract, col. 2 ll. 35–40.
- “In transactions in which a user communicates with a remote transaction partner via a communication channel such as the Internet, it is important to assure that an individual that identifies itself as an authorised user is actually the person it alleges to be,” such as an online bank transaction. ’903 patent col. 1 ll. 15-23.

BACKGROUND

- The patent specification also describes several known authentication methods involving a user's mobile device:
  - GB 2398159 A discloses an authentication method of the type indicated above, wherein the authentication function prompts the user to confirm the transaction, and a corresponding confirmation signal is sent from the mobile device to the authentication device.
  - WO 2008/052592 A1 discloses a credit card system wherein a mobile device of the user is used for activating and deactivating the credit card.
  - WO 2007/072001 A1 discloses an authentication method wherein the authentication device responds to the transmission of the user identification with sending an authentication token to the terminal from which the transaction has been requested. This token may for example be encoded in a digital image to be displayed on a display of the terminal. The authentication function in the mobile device is configured to capture this digital image and send it back to the authentication device via the second communication channel. *Id.* at col. 1 ll. 30-46.

BACKGROUND


TWO-FACTOR AUTHENTICATION
user@account.com
123456
SIGN IN


9:41
Monday, September 28
Apple ID Sign In Requested
karina_cavanna@icloud.com
Your Apple ID is being used to sign in to an iPhone near Cupertino, CA.
Don't Allow
Allow
Apple ID
Apple ID Verification Code
Didn't Get a Code?
Cancel

BACKGROUND

- "[I]t can be confirmed that the person carrying the mobile device, e.g. a mobile telephone, is actually present at the location of the terminal from which the transaction has been requested. Thus, as long as the user is in control of his mobile device, the authentication method assures that no third party can fake the identification data of this user and perform any transactions in his place." *Id*. at col. 1 ll. 47-50.
- The patent seeks to "provide an authentication method that is easy to handle and can be carried out with mobile devices of low complexity," in which "the authentication function is normally inactive and is activated by the user only preliminarily for the transaction, said response from the second communication channel includes the information that the authentication function is active, and the authentication function is automatically deactivated." *Id*. at col. 1 ll. 54-63.

BACKGROUND

- The patent specification asserts a significant **reduction in complexity** because "the only activity that is required from the user for authentication purposes is to activate the authentication function at a suitable timing for the transaction … [and] [o]nce the active state of the authentication function has been detected, this function is returned into the inactive state." *Id.* at col. 1 l. 64 – col. 2 l. 5.
- Suitable timing involves ""predetermined time relation" in that "the authentication function is activated within a certain (preferably short) time window after the transmission of the user identification." *Id.* at col. 2 ll. 8–14.
- There is also **enhanced security** since the authentication function is normal *inactive* and authentication will fail "when a third party fraudulently identifies itself as the user in order to initiate a transaction." *Id.* at col. 2 ll. 15-19.

BACKGROUND

- Even if "the true user happens to activate the authentication function of his mobile device just in the right moment … the fraud could be detected because the user will only activate the authentication function when he wants to make a transaction himself … [and] the authentication device would detect a coincidence between one activation of the authentication function and two transaction requests (normally launched from different terminals)." *Id.* at col. 2 ll. 22-30.
- Further, "[i]t is a particular advantage of the invention that the mobile device *does not have to have any specific hardware* for capturing or outputting information (emphasis added)." Id. at col. 2 ll. 44–46.

BACKGROUND

- Thus, instead of requiring the user to input multiple authentication factors using multiple communication channels, the user's identity is verified by transmitting the user identification via a first communication channel and checking via a second communication channel that an authentication function is activated in the user's mobile device. *Id.* at col. 1 ll. 3–9.
- Checking for an activated authentication function replaces the manual entry of information for an authentication factor by the user.
  - the user may activate the authentication function by activating their mobile device, *Id.* at col. 2 ll. 56–60, or by activating an application on a mobile device, *see Id.* at col. 6 ll. 59–62.

BACKGROUND

1. A method of authenticating a user to a transaction at a terminal, comprising the steps of:

transmitting a user identification from the terminal to a transaction partner via a first communication channel,

providing an authentication step in which an authentication device uses a second communication channel for checking an authentication function that is implemented in a mobile device of the user,

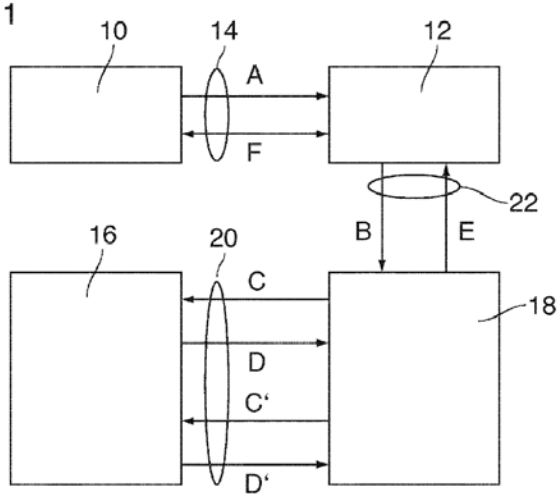
as a criterion for deciding whether the authentication to the transaction shall be granted or denied, having the authentication device check whether a predetermined time relation exists between the transmission of the user identification and a response from the second communication channel,

ensuring that the authentication function is normally inactive and is activated by the user only preliminarily for the transaction,

ensuring that said response from the second communication channel includes information that the authentication function is active, and

thereafter ensuring that the authentication function is automatically deactivated.

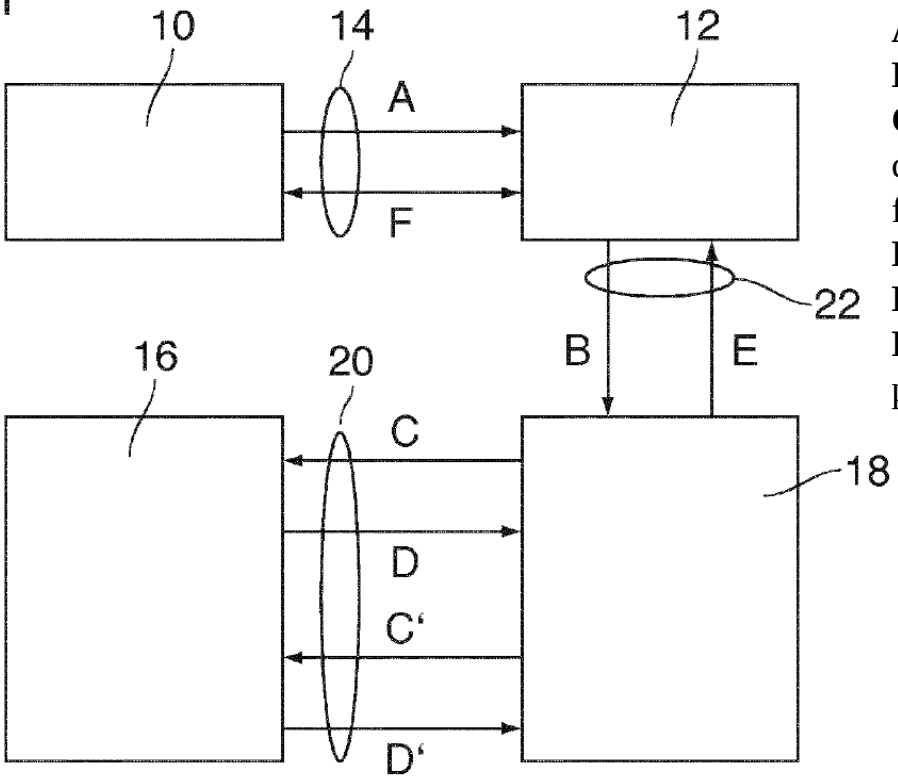
Fig. 1



- transaction terminal 10
- remote transaction partner 12
- first communication channel 14
- mobile device 16
- authentication device 18
- second communication channel 20 (mobile telephone network)

BACKGROUND

Fig. 1



A – transmitting the user-ID to 12
B – 12 forwards user-ID to 18
C – 18 retrieves mobile telephone # and contacts 16 or checks whether authentication function on 16 is active
D – confirms authentication function is active
E - 18 sends confirmation to 12
F – transaction between user and 12 to be performed

- transaction terminal 10
- remote transaction partner 12
- first communication channel 14
- mobile device 16
- authentication device 18
- second communication channel 20 (mobile telephone network)

BACKGROUND

Claim 1 Summary

1. Request from a terminal.
2. Checking authentication function implemented on user's mobile device *is active*.
3. Authentication function must be activated within predetermined time from the request.
4. Authentication function must normally be inactive and only activated by the user for the transaction.
5. Authentication function must automatically be deactivated after the transaction.

BACKGROUND -

- In September 2018, CosmoKey sued Duo Security, Inc. for infringement of the ’903 patent.
- In October 2019, Duo moved for judgment on the pleadings pursuant to Rule 12(c) of the Federal Rules of Civil Procedure, arguing that all claims of the ’903 patent are ineligible under 35 U.S.C. § 101 as the claims are directed to the abstract idea of authentication and do not recite any patent-eligible inventive concept.
- The district court granted Duo’s motion on June 24, 2020. At step one of the *Alice* two-step framework for determining patent eligibility, the district court agreed with Duo that the claims of the ’903 patent “are directed to the abstract idea of authentication—that is, the verification of identity to permit access to transactions.”

BACKGROUND – DC - *ALICE* STEP 1

- The district court reasoned that the "[']903 patent is not materially different from the patent at issue in *Prism Tech[nologies] LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014 (Fed. Cir. 2017)," where we determined that the patent claims were invalid because they were "directed to the abstract idea of 'providing restricted access to resources.'"
  - Link
- The district court determined that, "[g]iven the similarities between the abstract processes in the [']903 patent and the patent in *Prism*, … the claims at issue here are directed to the abstract idea of verifying identity to permit access to transactions." *Id.* at 678.

BACKGROUND – DC – *ALICE* STEP 2

- At *Alice* step two, the district court concluded that "the [']903 patent merely *teaches generic computer functionality* to perform the abstract concept of authentication; and it therefore fails *Alice*'s step two inquiry (emphasis added)." *Id.* at 678.
- The district court determined that the patent itself admits that "the detection of an authentication function's activity and the activation by users of an authentication function within a pre-determined time relation were **well-understood and routine, conventional activities** previously known in the authentication technology field (emphasis added)." *Id.* at 679 (citing '903 patent col. 1 ll. 15–53). (i.e., slides 3 and 4 above).

DISCUSSION

- The Federal Circuit applied regional circuit law (Third Circuit) to review the district court's grant of Duo's motion for judgement on the pleading de novo, "accepting as true all facts pleaded by CosmoKey and drawing all reasonable inferences in favor of CosmoKey."
- Supreme Court two-step test under 35 U.S.C. § 101:
  1. Step One: "determine whether the claims at issue are directed to a patent-ineligible concept[,]" such as an abstract idea. *Alice*, 573 U.S. at 218. If so…
  2. Step Two: "consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Id.* (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 78–79 (2012)).

DISCUSSION

- Step two is "a search for an 'inventive concept' (quoting *Mayo*, 566 U.S. at 72–73).
- *Prism* (U.S. 8,127,345 and U.S. 8,387,155)
  - The claims at issue were directed to the abstract idea of "providing restricted access to resources" because the claims did not cover a "concrete, specific solution." 696 F. App'x at 1017.
  - The claims recited generic steps typical of any conventional process for restricting access, independent claim of the '345 patent is summarized below:
    - Receiving identity data associated with client computer;
    - Authenticating the identity data;
    - Authorizing the client computer; and
    - Permitting access to the client computer.

DISCUSSION

- *Prism*
  - At step two, the Federal Circuit determined that the asserted claims recited *conventional generic computer components employed in a customary manner* such that they were insufficient to transform the abstract idea into a patent-eligible invention. *Id.* at 1017–18.
- In *Universal Secure Registry LLC v. Apple, Inc.*, 10 F.4th 1342 (Fed. Cir. 2021), the Federal Circuit held that the patent claims were directed to the abstract idea of combining multiple conventional authentication techniques for verifying the identity of a user to facilitate a financial transaction.
  - Includes biometric and multi-factor authentication, and using multiple devices, such that the claims were simply directed to combining these long-standing, well-known authentication techniques to achieve the expected result of increased security no greater than the sum of the security provided by each technique alone.

DISCUSSION

- In *Universal Secure Registry*
  - Under *Alice* step two, the Federal Circuit held that these claims did not recite an inventive concept because the combination of long-standing conventional methods of authentication yielded expected results of an additive increase in security, and nothing in the record suggested an additional technological improvement.
- In contrast, claims directed to *specific verification methods* that depart from earlier approaches and *improve computer technology* eligible under § 101.
  - In *Ancora Technologies Inc. v. HTC America, Inc.*, the Federal Circuit held that claims directed to storing a verification structure in computer memory were directed to a specific non-abstract computer-functionality improvement addressing the "vulnerability of license-authorization software to hacking." 908 F.3d 1343, 1348–49 (Fed. Cir. 2018).

DISCUSSION

- *Ancora*
  - "[i]mproving security . . . can be a non-abstract computer-functionality improvement if done by *a specific technique* that departs from earlier approaches to solve a specific computer problem (emphasis added)." *Id.* at 1349.
  - the claims "yield[ed] a *tangible technological benefit* (emphasis added)" in making the system less susceptible to hacking by altering how the verification is performed. *Id.* at 1350.
- *Alice* Step One
  - The Federal Circuit considers "what the patent asserts to be the 'focus of the claimed advance over the prior art.'" *Solutran, Inc. v. Elavon, Inc.*, 931 F.3d 1161, 1168 (Fed. Cir. 2019).

DISCUSSION

- The district court held that the claims "are directed to the abstract idea of authentication—that is, the verification of identity to permit access to transactions." *Judgment Op.*, 468 F. Supp. 3d at 677.
- The Federal Circuit disagreed with this broad characterization.
- Instead, the focus of the claimed advance is activation of the authentication function, communication of the activation within a predetermined time, and automatic deactivation of the authentication function, such that the invention provides enhanced security and low complexity with mini-mal user input.
- The critical question is whether this corrected characterization of the claims is either an abstract idea or a specific improvement in computer verification and authentication techniques. *Ancora*, 908 F.3d at 1347.

DISCUSSION

- Skipped Step One analysis, and went directly to Step Two.
- Turning then to *Alice* step two, we "consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Alice*, 573 U.S. at 217 (quoting Mayo, 566 U.S. at 77–78).
- In computer-implemented inventions, the tine, conventional activities previously known to the industry … and cannot simply be an instruction to implement or apply the abstract idea on a computer."

DISCUSSION

- The district court held that the ’903 patent failed at step two because it “merely teaches generic computer functionality to perform the abstract concept of authentication[.]” *Judgment Op.*, 468 F. Supp. 3d at 678.
- As noted above, the district court cited column 1, lines 15-53 of the ‘903 Patent for admitting the claimed steps were well-understood, routine and conventional activities previously known.
- The Federal Circuit disagrees, as the ‘903 patent claims and specification recite a specific improvement to authentication that increases security, prevents unauthorized access by a third party, is easily implemented, and can advantageously be carried out with mobile devices of low complexity. *See* ’903 patent col. 2 ll. 15–32.
  - This amounts to a technical solution to a security problem in networks and computers.

DISCUSSION

- While authentication of a user's identity using two communication channels and a mobile phone was known at the time of the invention, there is no disclosure or support that last four steps of independent claim 1 of the '903 patent are conventional.
  - as a criterion for deciding whether the authentication to the transaction shall be granted or denied, having the authentication device check whether a **predetermined time relation exists** between the transmission of the user identification and a response from the second communication channel, (2) ensuring that the **authentication function is normally inactive** and is **activated by the user only preliminarily** for the transaction, (3) ensuring that said response from the second communication channel includes information that the **authentication function is active**, and thereafter (4) ensuring that the **authentication function is automatically deactivated.**
- The district court's reliance on column 1, lines 15–53 as allegedly admitting that these steps were routine or conventional is misplaced, as none of the references teach the steps noted above.

DISCUSSION

- In contrast, the specification describes the prior art references as disclosing: (1) sending a prompt to a user to confirm the transaction followed by the user's mobile device sending a confirmation signal; (2) using a user's mobile device for activating and deactivating a credit card; and (3) sending a token to the user's terminal from which a transaction has been requested followed by the user's mobile device capturing the image and sending it back to the authentication device via a second communication channel. Id. at col. 1 ll. 30–46.
- The claimed steps were developed by the inventors, are not admitted prior art, and yield certain advantages over the described prior art.

DISCUSSION

- The specification emphasizes the inventive nature of these steps, explaining that "the complexity of the authentication function can be reduced significantly" be-cause "the only activity that is required from the user for authentication purposes is to activate the authentication function at a suitable timing for the transaction." *Id.* at col. 1 l. 64–col. 2 l. 3.
- The specification ex-plains that compared to the prior art and conventional multifactor authentication systems, the '903 patent performs user authentication with fewer resources, less user inter-action, and simpler devices. *Id.* at col. 1 ll. 54–56
- Duo argues that using a second communication channel in a timing mechanism and an authentication function that is normally inactive, activated only preliminarily, and automatically deactivated is itself an abstract idea and thus cannot contribute to an inventive concept.

DISCUSSION

- The claim limitations are specific and recite an improved method for overcoming hacking by:
  - ensuring that the authentication function is normally inactive, activating only for a transaction, communicating the activation within a certain time window, and thereafter ensuring that the authentication function is automatically deactivated.
- The specification explains that these features in combination with the other elements of the claim constitute an improvement that increases computer and network security, prevents a third party from fraudulently identifying itself as the user, and is easy to implement and can be carried out even with mobile devices of low complexity. '903 patent col. 2 ll. 15–32.

DISCUSSION

- The claim limitations are specific and recite an improved method for overcoming hacking by:
  - ensuring that the authentication function is normally inactive, activating only for a transaction, communicating the activation within a certain time window, and thereafter ensuring that the authentication function is automatically deactivated.
- The specification explains that these features in combination with the other elements of the claim constitute an improvement that increases computer and network security, prevents a third party from fraudulently identifying itself as the user, and is easy to implement and can be carried out even with mobile devices of low complexity. '903 patent col. 2 ll. 15–32.

DISCUSSION

- We recognized in *Ancora* that improving computer or network security can constitute "a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem." 908 F.3d at 1349.
- Here, as the specification itself makes clear, the claims recite an inventive concept by requiring a specific set of ordered steps that go beyond the abstract idea identified by the district court and improve upon the prior art by providing a simple method that yields higher security.

Conclusion

- Reversed the district court's judgment that the asserted claims of the '903 patent are ineligible under § 101.

REYNA – CONCURRING OPINION

- Concludes under ***Alice*** **step one**, the subject claims are directed to patent-eligible subject matter.
- The majority skips step one of the Alice inquiry and bases its decision on what it claims is step two.
- Determines that *Alice* does not provide a basis for skipping the first step or for conflating the two steps into one.
- The *Alice* inquiry should be viewed as a loose filter that prevents the patenting of abstract ideas.
- To this end, step one serves several important purposes, chief among them being that a patent must lay bare that which is claimed.

REYNA – CONCURRING OPINION

- At step one, we examine whether the claim is directed to patent-ineligible subject matter. Among other things, this examination permits us to distinguish between claims that recite mere concepts, functions or results (abstract ideas) from those that, through claimed limitations, chart the specific means for achieving such concepts, functions or results. *Ancora Techs., Inc. v. HTC Am., Inc.*, 908 F.3d 1343, 1347 (Fed. Cir. 2018).
- For example, generally, if a claim is directed to a specific technological solution to a technological problem, it is not directed to an abstract idea. *See Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1336 (Fed. Cir. 2016).

REYNA – CONCURRING OPINION

- Our precedent is clear that once a claim is deemed not directed to an abstract idea, the *Alice* inquiry ends. We do not proceed to step two. *Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc.*, 880 F.3d 1356, 1361 (Fed. Cir. 2018).
- Step two does not operate independently of step one but comes into play only when a claim has been found to be directed to patent-ineligible subject matter.
- The step two inquiry recognizes that the claim has been struck down as ineligible.
- The question is whether there is any reason to save the claim on the basis of whether additional elements of the claim, considered individually and as an ordered combination, transform the nature of the claim into a patent-eligible application of the abstract idea. *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat'l Ass'n*, 776 F.3d 1343, 1347 (Fed. Cir. 2014) (citing *Al-ice*, 573 U.S. at 217).

REYNA – CONCURRING OPINION

- Employing step one, Reyna concludes that the claims at issue are directed to patent-eligible subject matter.
- Reyna agrees that "[t]he '903 Patent claims and specification recite *a specific improvement to authentication* that in-creases security, prevents unauthorized access by a third party, is easily implemented, and can advantageously be carried out with mobile devices of low complexity." Majority Op. 11-12 (emphasis added).
- But this is a step-one rationale. *See Enfish*, 822 F.3d at 1336 ("[T]he first step in the *Alice* inquiry in this case asks whether the focus of the claims is on the specific asserted *improvement in computer capabilities* . . . or, instead, on a process that qualifies as an 'abstract idea' for which computers are invoked merely as a tool (emphasis added)."); *McRO*, 837 F.3d at 1314

CONCLUSION

- We should not lose sight, as my colleagues have in this case, that the "question of abstraction is whether the claim is 'directed to' the abstract idea itself." *Data Engine Techs. LLC v. Google LLC*, 906 F.3d 999, 1011 (Fed. Cir. 2018).

- In Summary, the '903 Patent provides an improved and *novel* authentication process that is utilizes an authentication function that is normally *inactive* and is activated by a user, on the user's mobile terminal, within a "predetermined time relation" and is automatically deactivated.
  - It has the advantageous properties of permitting a reduction in complexity for the user, who only has to activate the authentication function and not perform any confirmation of an authentication prompt sent to the user (GB 2398159), or requiring the generation, by an authentication device of a terminal, of a token embedded in an image and an authentication function on a user's mobile terminal that captures the digital image and sends it back to the authentication device.

CONCLUSION

- Thus, the improvement here is to the method of authenticating, which simplifies the process and improves security.
- That is, in this case, there is an improvement to the process executed by a computer systems (i.e., the terminal, the remote transaction partner, the authentication device, and the mobile terminal) but there is no actual improvement to the computer systems themselves.

- Any Questions or Comments?