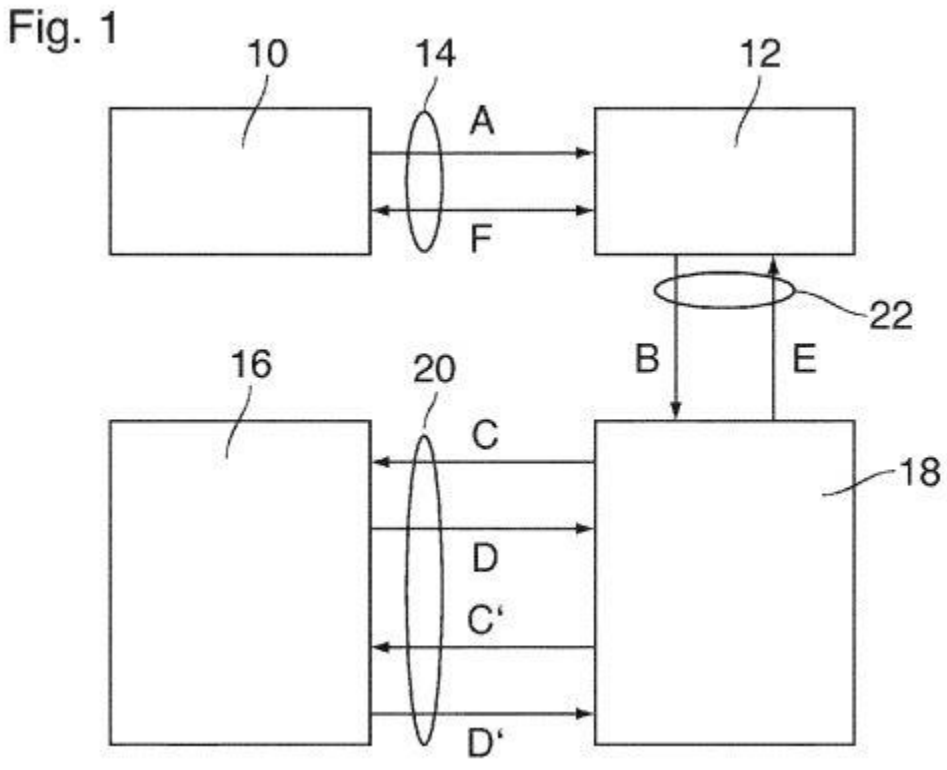
Eligibility: Turning Application On-and-Off for Authentication Patent Eligible

October 6, 2021Dennis Crouch
by Dennis Crouch

CosmoKey Solutions v. Duo Security (Fed. Cir. 2021)

Patentee wins this one–with the Federal Circuit reversing the district court and finding the claims on patent-eligibility under *Alice* step-two. This is another case that serves as a data-point, but I struggle to differentiate it from similar cases finding claims ineligible.

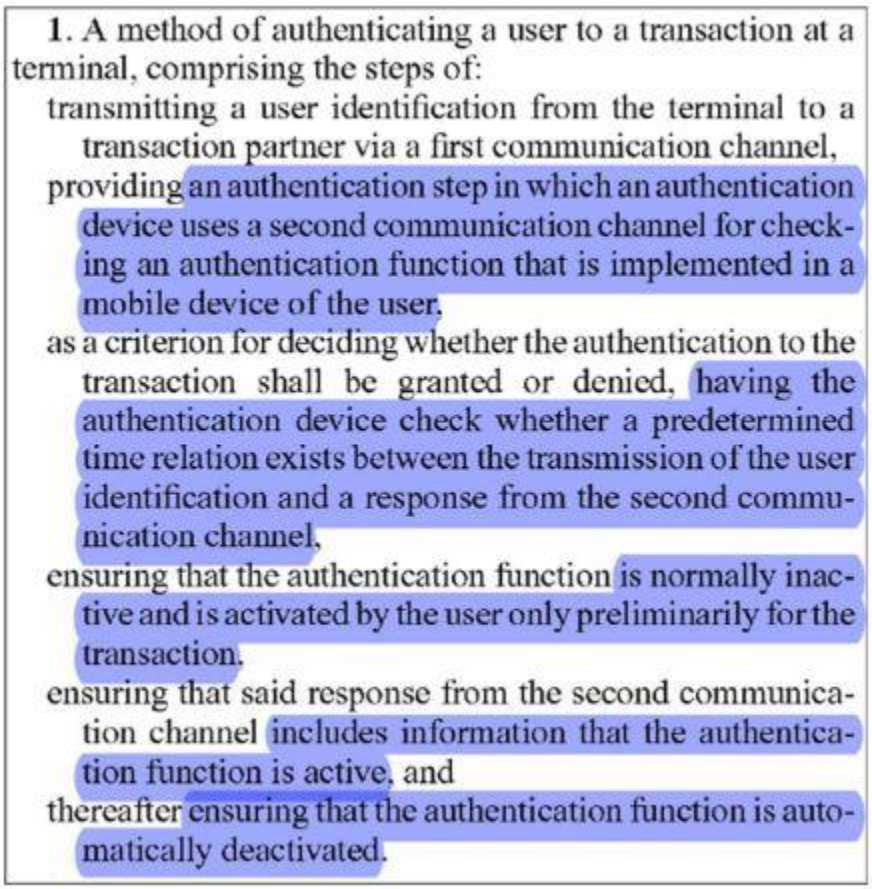


CosmoKey's U.S. Patent No. 9,246,903 is directed a low-complexity, high-security method of authenticating a user transaction. (2011 priority filing date). The basic idea here is two-factor-authentication that uses a second communication channel (mobile phone) to authenticate a

transaction. This general idea was already in the prior art, but the claims add a couple of additional features:

- Authentication function is normally inactive on the mobile device but is activated by the user for the transaction; and when once the transaction is done the authentication function is automatically deactivated. This on/off function is designed to both save power on the device and also help prevent hacking.
- As part of the authentication, there is a check on how long the user takes to respond (whether a predetermined time relation exists between the transmission of the user identification and a response from the second communication channel);

See '903 Patent Claim 1.



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.

The district court found the claim ineligible under Section 101 after finding them closely parallel to the authentication method claims invalided in *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014 (Fed. Cir. 2017) (nonprecedential opinion). In particular, the district court found the claims directed to "the abstract idea of authentication—that is, the verification of identity to permit access to transactions" (*Alice* Step 1) and that the claims recite generic computer functionality that were all well understood, routine, and conventional activities at the time of the invention (*Alice* Step 2).

On appeal, the Federal Circuit has reversed — holding that the patent "discloses a technical solution to a security problem in networks and computers." That statement suggests reversal on *Alice* Step 1; but the court actually leapt to Step 2 without a clear holding on Step 1. Here, the court found that the claimed steps were (1) developed by the inventors; (2) not admitted prior art; and (3) yield advantages over the described prior art. The court noted the difficulty with this case — the purpose of the invention was to "reduce significantly" "the complexity of the authentication function." But, simplification can quickly suggest abstraction.

Eligibility Jurisprudence: It has been quite difficult to nail down the meaning of "abstract idea." The Supreme Court suggested that we look back to prior cases to find the answer, and that is the same approach that has been followed by the lower courts as well as the USPTO. Here, however, the Federal Circuit cautioned that analysis:

While prior cases can be helpful in analyzing eligibility, whether particular claim limitations are abstract or, as an ordered combination, involve an inventive concept that transforms the claim into patent eligible subject matter, must be decided on a case-by-case basis in light of the particular claim limitations, patent specification, and invention at issue. Here, the claim limitations are more 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.

Slip Op.

The court's opinion was written by Judge Stoll and joined by Judge O'Malley. Judge Reyna penned a concurring opinion arguing that the two step Alice approach should be taken in-order:

The majority skips step one of the Alice inquiry and bases its decision on what it claims is step two. I believe this approach is extraordinary and contrary to Supreme Court precedent. It turns the Alice inquiry on its head.

Concurring Opinion. Judge Reyna goes on to explain how Step 2 should be seen as a "lifeline" that only comes into play to save claims that are directed toward abstract ideas. But, we can't know if there is "something more" without first answering the question "more than what."

Step two is rendered superfluous and unworkable without step one. Without the benefit of a step-one analysis, we are hobbled at step two in reasonably determining whether additional elements transform the nature of the claim into a patent-eligible application of the abstract idea. And by skipping step one, we create a risk that claims that are not directed to an abstract idea might be deemed to "fail" at
step two.

Id. Judge Reyna then goes on to conclude that the claims are not directed to an abstract idea. Id. Quoting the majority statement that "the 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."