

ABSTRACT**METHOD, DEVICE, SERVER AND SYSTEM FOR AUTHENTICATING A USER**

The invention relates to a method 40 for authenticating a user.

5 According to the invention, the method comprises the following steps. A device 12 accesses 41 a key and at least one initial vector. The key is a single use key and is not dependent on user authentication data. The at least one initial vector is previously generated by using a first algorithm, at least one reference vector and reference user authentication data. The at least one reference vector is previously generated without
10 using the reference user authentication data. The device accesses data 42 and provided user authentication data 46. The device generates 48 at least one intermediary vector by using a second algorithm, the at least one initial vector and the provided user authentication data. The device generates 410 a cryptogram by using a third algorithm 22, the key, the at least one intermediary vector and the data. A server 18 receives a
15 request 414 for authenticating a user accompanied with the cryptogram and the data. The server accesses 416 the key and the at least one reference vector. The server generates 418 a reference cryptogram by using the third algorithm, the key, the at least one reference vector and the data. The server verifies 420 whether the reference cryptogram does or does not match the cryptogram. If the reference cryptogram does or
20 does not match the cryptogram, then the server does 422 or does not 424 authenticate the user respectively.

The invention also relates to corresponding device, server and system.

Figure 4